(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年4 月7 日 (07.04.2005)

PCT

(10) 国際公開番号
WO 2005/031560 A1

(51) 国際特許分類[7]: G06F 3/12

(21) 国際出願番号: PCT/JP2004/013956

(22) 国際出願日: 2004 年9 月24 日 (24.09.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-333268 2003 年9 月25 日 (25.09.2003) JP
特願2004-050848 2004 年2 月26 日 (26.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 大日本印刷株式会社 (DAI NIPPON PRINTING CO., LTD.) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 姉川 武彦 (ANEGAWA, Takehiko) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内 Tokyo (JP). 矢野 義博 (YANO, Yoshihiro) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内 Tokyo (JP).

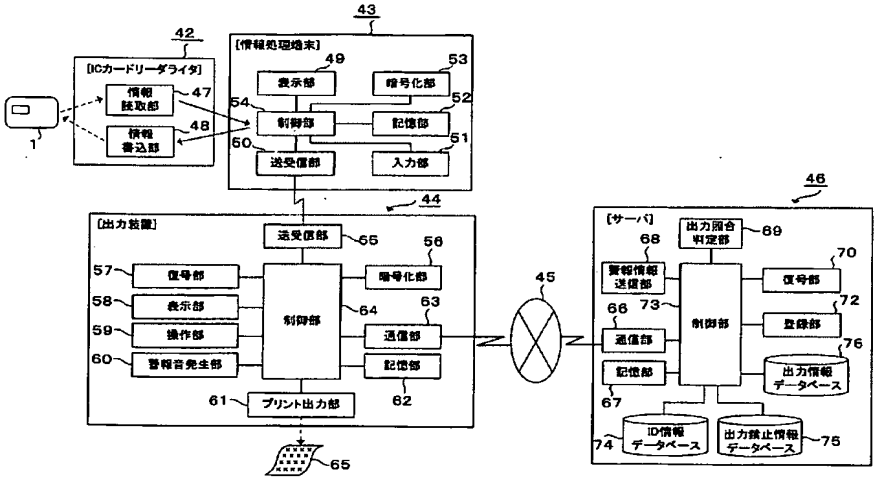
(74) 代理人: 中村 聡延, 外(NAKAMURA, Toshinobu et al.); 〒1040031 東京都中央区京橋一丁目１６番１０号 オークビル京橋４階 東京セントラル特許事務所内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA,

[続葉有]

(54) Title: OUTPUT INFORMATION MANAGEMENT SYSTEM

(54) 発明の名称: 出力情報管理システム



42... IC CARD READER/WRITER
47... INFORMATION READING PART
48... INFORMATION WRITING PART
43... INFORMATION PROCESSING TERMINAL
49, 58... DISPLAY PART
54, 64, 73... CONTROL PART
50... TRANSMITTING/RECEIVING PART
53, 56.. ENCRYPTING PART
52, 62, 67... STORING PART
51... INPUTTING PART
44... OUTPUTTING APPARATUS
55... TRANSMITTING/RECEIVING PART
57, 70... DECRYPTING PART
59... OPERATING PART
60... WARNING SOUND GENERATING PART
61... PRINT OUTPUTTING PART
63... COMMUNICATING PART
46... SERVER
69... OUTPUT COLLATING PART
68... WARNING SOUND INFORMATION TRANSMITTING PART
66... COMMUNICATING PART
74... ID INFORMATION DATABASE
72...REGISTERING PART
76...OUTPUT INFORMATION DATABASE
75... OUTPUT INHIBITION INFORMATION DATABASE

(57) Abstract: An output information management system and a method therefor wherein an output apparatus, which outputs information to a medium, can be prevented from being used by a third person and an effective examination can be performed for unauthorized use of even a person who has an authorized usage

[続葉有]

WO 2005/031560 A1

NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

right. A server, which constitutes the output information management system, associates ID information stored in a user IC card with information that is outputted by the output apparatus into a medium and stores those information into an output information database. According to this system, even if unauthorized use is performed in output, it leaves a specific evidence that shows who uses the output apparatus to output which information. In this way, unauthorized use can be prevented, and an effective examination can be performed even after performance of unauthorized use.

(57) 要約: 媒体に情報を出力する出力装置が、第三者により使用されることを防止すると共に、正規に使用権限を有する者の不正行為に対しても、調査を効率的に行えるようにした出力情報管理システム及びその方法を提供する。出力情報管理システムを構成するサーバは、利用者用のＩＣカードに記憶されているＩＤ情報と、出力装置が媒体に出力する情報とを関係付けて出力情報データベースに記憶する。これによれば、出力において不正行為が行われた場合でも、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残る。よって、不正行為を事前に予防すると共に、不正行為が行われた場合の調査を効率的に行うことができる。

明 細 書

出力情報管理システム

技術分野

[0001] 本発明は、媒体に情報を出力する機能を有する複写機やプリンタなどの出力装置により、重要情報などが不正に媒体に出力されて情報の漏洩が行われることを防止すると共に、たとえ不正な出力が行われた場合でも、その情報を出力した者を特定可能とした出力情報管理システムに関する。

背景技術

[0002] 従来、紙媒体に情報を出力する機能を有する複写機やプリンタなどの出力装置において、第三者が出力装置を使用して、不正に重要情報を紙媒体に出力して持ち出すといった情報の漏洩や、使用権限を有しない第三者による出力装置の無断使用などを防止することが必要とされている。このため、正規の使用権限を有する利用者が、管理用のカード等の情報記憶媒体を所持し、出力装置を使用する際にこれらの情報記憶媒体を用いて本人照合などを行うことで、出力装置の利用管理を行う場合がある。

[0003] これら管理用のカード等の情報記憶媒体を用いた利用者の制限に関する従来の技術は、既に公知となっているものがある(例えば、特許文献1及び2参照)。

[0004] しかしながら、これら従来の出力装置に関する使用管理では、管理用のカード等の情報記憶媒体を所持する使用権限を有する者以外の第三者による出力装置の使用を防止することはできるが、仮に、正規に出力装置の使用権限を有する者自身が、出力装置を用いて不正に重要情報を紙媒体に出力させて盗むなどの不正行為を行ったとした場合には、その不正行為を防止することはできないという問題がある。

[0005] また、この場合には、その不正行為が行われたという証拠も無いことが多く、内部の者による不正行為に対してのセキュリティ上の予防が図られにくく、従来の技術ではセキュリティ効果がほとんどないという問題がある。

[0006] したがって、従来の不正防止技術では、正規に出力装置の使用権限を有する者に対しての不正防止効果はなく、不正行為を行うか否かは、正規に出力装置の使用権

限を有する者のモラルを信用するしかないという状況である。

[0007] 特許文献1:特開2000−10441号公報

特許文献2:特開2000−98833号公報

発明の開示

発明が解決しようとする課題

[0008] 本発明は、媒体に情報を出力する機能を有する出力装置が、使用管理用のカード等の情報記憶媒体を所持する使用権限を有する者以外の第三者により使用されることを防止することが可能な出力情報管理システムを提供することを課題とする。

[0009] 更に、本発明は、正規に出力装置の使用権限を有する者により、不正に重要情報を媒体に出力させて盗むなどの不正行為が行われた場合でも、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残るようにして、不正行為の事前予防と、不正行為が行われた場合の調査が効率的に行えるようにした出力情報管理システムを提供することを課題とする。

課題を解決するための手段

[0010] 本発明の1つの観点では、利用者用の情報記憶媒体と、媒体に情報を出力する出力装置と、前記出力装置と通信回線を介して通信可能に接続されているサーバとからなる出力情報管理システムであって、前記情報記憶媒体には、固有情報が記憶された記憶部が設けられ、前記出力装置には、前記情報記憶媒体から固有情報を読み取る読取部と、媒体に出力する情報を前記読取部で読み取った固有情報と関係付けた情報として、前記サーバに送信する手段とを有し、前記サーバには、前記出力装置から受信した固有情報と関係付けられた情報を記憶させておくデータベースを有する。

[0011] また、媒体に情報を出力する出力装置と通信回線を介して接続されているサーバであって、前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されたデータベースと、前記出力装置から、前記媒体に出力する出力情報と、前記利用者の固有情報とを受信する受信部と、前記出力装置から受信した出力情報と固有情報とを関係付けてデータベースに記憶する記憶部と、前記出力装置から受信した出力情報を、前記データベースに登録

されている情報と照合する照合部と、前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置または管理者用情報処理端末に警報情報を送信する手段あるいは出力動作を止める手段とを有する。

[0012] 上記のように構成された出力情報管理システムまたはサーバは、利用者用の情報記憶媒体に記憶されている固有情報と、出力装置が媒体に出力する情報とを関係付けてデータベースに記憶する。これによれば、出力において不正行為が行われた場合でも、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残る。よって、不正行為を事前に予防すると共に、不正行為が行われた場合の調査を効率的に行うことができる。

[0013] 上記出力情報管理システムの一態様では、前記サーバには、前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されたデータベースと、前記出力装置から受信した情報を前記データベースに登録されている情報と照合する照合部と、前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置または管理者用情報処理端末に警報情報を送信する手段あるいは出力動作を止める手段を備えている。これによれば、出力情報管理システムは、出力禁止情報または出力許可情報が登録されているデータベースに基づいて、出力装置で出力してよい情報であるか否かを的確に判定することができる。

[0014] 上記出力情報管理システムの他の一態様では、前記データベースは、前記出力装置毎に前記出力禁止情報、または前記出力許可情報が登録されており、前記照合部は、前記出力装置から受信した情報を、当該出力装置に対応する前記出力禁止情報、または当該出力装置に対応する前記出力許可情報と照合する。これによれば、出力装置の設置場所に基づいて、利用者が出力しようとしている情報を判定することができる。例えば、所定の部署が所属する各フロアに1台ずつ出力装置が設置されている場合、利用者は自分が所属するフロアに設置された出力装置からのみ出力可能とすることができる。このように、出力装置毎に出力を許可するか否かを判定することで、特に、各フロアでそれぞれ異なる顧客の機密情報を扱っている場合に、情報漏

洩を防止すると共にセキュリティの向上を図ることができる。

[0015] 本発明の別の観点では、出力情報管理方法は、利用者が所持する情報記憶媒体と、媒体に情報を出力する出力装置と、前記出力装置と通信回線を介して通信可能に接続されているサーバとからなる出力情報管理システムにおける出力情報管理方法であって、前記出力装置が、前記情報記憶媒体の記憶部に記憶された固有情報を読み取るステップと、前記出力装置から前記サーバに、前記出力装置で出力した情報を前記固有情報と関連付けた情報として送信するステップと、前記サーバで受信した前記固有情報と関連付けられた情報を、前記サーバのデータベースに記憶させるステップと、からなる。

[0016] 上記のような出力情報管理方法をコンピュータ上で実施することにより、上述の出力情報管理システムと同様の効果を得ることができる。

[0017] 本発明の別の観点では、情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを備えた情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、前記出力装置と通信可能に接続されているサーバと、からなる出力情報管理システムであって、前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記出力装置に送信する手段とを有し、前記出力装置は、前記情報処理端末から受信したID情報と出力情報とを前記サーバに送信する手段を有し、前記サーバは、前記出力装置から受信したID情報と出力情報とを関係付けてデータベースに記憶させる手段を有する。

[0018] 上記のように構成された出力情報管理システムでは、利用者が使用する情報処理端末が出力装置により紙媒体に出力する情報を、当該利用者のID情報に関係付けてデータベースに記憶させることができる。つまり、これによれば、情報処理端末による出力において不正行為が行われた場合でも、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残る。よって、不正行為を事前に予防すると共に、不正行為が行われた場合の調査を効率的に行うことができる。

[0019] 本発明の別の観点では、情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを備えた情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記出力装置と通信可能に接続されているサーバと、前記サーバを介して前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、からなる出力情報管理システムであって、前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記サーバに送信する手段とを有し、前記サーバは、前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、前記情報処理端末から受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信する出力情報送信部と、を有する。

[0020] また、情報を紙媒体に出力する出力装置と通信可能に接続されているサーバであって、前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、利用者を特定可能なID情報と、前記紙媒体に出力する出力情報とを受信する受信部と、前記受信部が受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信する出力情報送信部と

、前記受信部が受信したID情報と、前記照合部による照合の結果、前記出力禁止情報と不一致となった出力情報、または前記出力許可情報と一致した出力情報とを関係付けて出力情報データベースに記憶させる。

[0021] 上記のように構成された出力情報管理システムまたはサーバは、利用者が紙媒体に出力しようとしている情報が禁止されているものであるか否かを出力判定情報データベースを参照することにより的確に判定することができる。そして、当該情報の出力が禁止されている場合、出力装置に警報情報を送信することで利用者に出力できない旨を伝える。これによれば、利用者が出力装置により情報を出力する前に、当該情報の出力が禁止されているものであれば、出力動作を停止させることができる。よって、情報漏洩を防止すると共に、セキュリティの向上を図ることができる。

[0022] 上記出力情報管理システムの一態様では、サーバは、前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、前記情報処理端末から受信したID情報と、前記照合部による照合の結果、前記出力禁止情報と不一致となった出力情報、または前記出力許可情報と一致した出力情報とを関係付けて出力情報データベースに記憶させる手段と、をさらに有する。これによれば、たとえ出力判定情報データベースに登録されていないが、出力を禁止する情報が出力されてしまったとしても、出力情報データベースを参照することにより、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残る。よって、不正行為を事前に予防すると共に、不正行為が行われた場合の調査を効率的に行うことができる。

[0023] 本発明のさらに別の観点では、情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを備えた情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記出力装置と通信可能に接続されている処理サーバと、前記処理サーバが出力を許可した情報を記憶する保管サーバと、前記処理サーバを介して前記情報処理端末から受信した情報を紙媒体に出力する出力装置とからなる出力情報管理システムであって、前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、前記情報処理端末は、前記リーダライタ

で読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記処理サーバに送信する手段とを有し、前記処理サーバは、前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、前記情報処理端末から受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信し、前記出力情報及びID情報を前記保管サーバに送信する送信部とを有し、前記保管サーバは、前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、前記処理サーバから受信したID情報と出力情報とを関係付けて前記出力情報データベースに記憶させる手段と、をさらに有する。

[0024] 上記のように構成された出力情報管理システムによれば、利用者が出力しようとする情報が禁止されているか否かを判定する処理サーバと、利用者を特定するID情報と出力情報とを関係付けて記憶する保管サーバとが別々のサーバとなっている。これにより、出力情報の判定は1箇所に集約された処理サーバで効率的に行うとともに、メモリを多く消費する出力情報の記憶は複数箇所に設置された保管サーバで行うことが可能となる。

[0025] 上記出力情報管理システムの一態様では、前記出力判定情報データベースは、前記出力装置毎に前記出力禁止情報、または前記出力許可情報が登録されており、前記照合部は、前記情報処理端末から受信した情報を、出力を予定している出力装置に対応する前記出力禁止情報、または当該出力装置に対応する前記出力許可情報と照合する。これによれば、出力装置毎に、例えば出力装置の設置場所などに基づいて、利用者が出力しようとしている情報を判定することができる。

[0026] 上記出力情報管理システムの他の一態様では、前記情報記憶媒体は、ICカードであることを特徴とする。

発明の効果

[0027] 本発明の出力情報管理システムは、出力装置が使用される際に、利用者が所持する情報記憶媒体による固有情報の照合処理を行うと共に、出力装置の利用者を特定可能な情報と、複写又は出力情報などの情報とを関係付けてデータベースに登録しておくので、使用権限の無い利用者による出力装置の使用を防止でき、更に正規の使用権限を有する者が不正行為を行ったとしても、誰が、どのような内容の複写を行ったのかについてデータベースを調べることで、簡単に調査することができるという効果がある。

[0028] また、本発明の出力情報管理システムは、パソコンなどの情報処理端末からプリンタなどの出力装置に送信されてきた情報を、出力装置により紙媒体に出力する際に、出力装置で出力した情報と、利用者を特定可能なID情報とを関係付けてサーバ側のデータベースに記憶させておくので、正規の使用権限を有する者が不正行為を行ったとしても、誰が、どのような内容のプリント出力を行ったのかをデータベースに記憶された情報を調べることで、簡単に調査することができるという効果がある。

[0029] また、本発明の出力情報管理システムは、利用者が出力装置により情報を出力する前に、当該情報の出力が禁止されているものであれば、出力動作を停止させることができる。即ち、情報漏洩を防止すると共に、セキュリティの向上を図ることができるという効果がある。

[0030] また、本発明の出力情報管理システムは、出力情報の判定は1箇所に集約された処理サーバで効率的に行うとともに、メモリを多く消費する出力情報の記憶は複数箇所に設置された保管サーバで行うことができるという効果がある。

図面の簡単な説明

[0031] [図1]本発明の第1実施形態に係る出力情報管理システムの概要を説明する図である。

[図2]第1実施形態に係る出力情報管理システムのシステムブロック図である。

[図3]禁止情報リストの構造を模式的に示す図である。

[図4]社員の属性等に基づく出力制限テーブルの構造を模式的に示す図である。

[図5]プリンタ設置場所に基づく出力制限テーブルの構造を模式的に示す図である。

[図6]第1実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[図7]第1実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[図8]第2実施形態に係る出力情報管理システムの概要を説明する図である。

[図9]第2実施形態に係る出力情報管理システムのシステムブロック図である。

[図10]第2実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[図11]第2実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[図12]第3実施形態に係る出力情報管理システムの概要を説明する図である。

[図13]第3実施形態に係る出力情報管理システムのシステムブロック図である。

[図14]第3実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[図15]第4実施形態に係る出力情報管理システムの概要を説明する図である。

[図16]第4実施形態に係る出力情報管理システムのシステムブロック図である。

[図17]第4実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

符号の説明

[0032]
1 ICカード
2 複写機
3 サーバ
4 通信回線
5 カード情報読取部
6 操作部
7 複写情報読取部
8 デジタル情報変換部
9 表示部

10　複写部

11、18　記憶部

12、22　通信部

13、19　制御部

発明を実施するための最良の形態

[0033] 以下、本発明の実施形態に係る出力情報管理システムについて図面に基づいて詳細に説明する。

第1実施形態

[0034] 図1乃至図7を参照して、本発明の第1実施形態について説明する。図1は、本発明の第1実施形態に係る出力情報管理システムの概要を説明するための図である。図2は、本発明の第1実施形態に係る出力情報管理システムのシステムブロックである。図3は、禁止情報リストの構造を模式的に示す図である。図4は、社員の属性に基づく出力制限テーブルである。図5は、複写機設置場所に基づく出力制限テーブルである。図6及び図7は、本発明の第1実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[0035] [出力情報管理システム]

まず、図1及び図2を参照して出力情報管理システムの概要について説明する。

[0036] 本発明の第1実施形態に係る出力情報管理システムは、図1に示すように、利用者用の情報記憶媒体であるICカード1と、紙媒体に情報を表示させて出力する出力装置である複写機2と、複写機2と通信回線4を介して通信可能に接続されている管理用のサーバ3とから構成されている。

[0037] 情報記憶媒体であるICカード1には、固有情報であるID情報が記憶されたメモリからなる記憶部が設けられている。

[0038] 複写機2には、ICカード1の記憶部に記憶されている固有情報であるID情報を読み取るカード情報読取部5と、利用者が指示情報の入力を行うなどの操作をするための操作部6と、複写する原稿をスキャンしてその表示内容をイメージ情報として読み取る複写情報読取部7と、この複写情報読取部7で読み取ったイメージ情報をデジタル情報に変換するデジタル情報変換部8と、表示部9と、紙媒体に対して原稿の内容

を複写して表示出力する複写部10と、記憶部11と、通信回線4を介してサーバ3と送受信を行う通信部12と、制御部13と、警報音発生部25とが備えられている。

[0039] また、サーバ3には、通信回線4を介して複写機2と送受信を行う通信部22と、ICカード1の記憶部に記憶されているID情報を複写機2から受信した際に、照合処理を行うために予め照合用のID情報が登録されているID情報データベース14と、複写機2からコピーとして複写出力された内容をデジタルデータとして、ID情報と関連付けた状態で記憶させておく出力情報データベース15と、複写機2から受信したID情報と、ID情報データベース14に予め登録されているID情報とを照合する照合部16と、複写機2から受信したID情報と複写情報とを関係付けた状態として出力情報データベース15に登録する登録部17と、記憶部18と、制御部19と、出力判定情報データベース23と、出力照合判定部24とを有している。

[0040] ID情報データベース14に予め登録されている情報としては、ID情報と関係付けられた状態で、氏名、所属、などの利用者である個人を特定できる情報が登録されている。

[0041] このID情報は、例えば社員番号などのように、予め組織上における管理用の個人識別番号と同一番号を定めておいてもよく、これにより、他のシステムと連動した情報システムの一部として管理を行うようにしてもよい。

[0042] また、出力判定情報データベース23には、出力装置である複写機2により、出力を禁止している出力禁止情報、または出力装置で出力を許可している出力許可情報が登録されている。

[0043] 出力照合判定部24は、出力装置である複写機2から受信した情報を出力判定情報データベース23に登録されている情報と照合する機能を有し、出力照合判定部24による照合の結果、出力禁止情報と一致した場合、または出力許可情報と不一致となった場合に、複写機2または通信端末26に警報情報を送信するか、あるいは出力動作を止めるように制御部19が制御する。ここで、通信端末26とは、例えば複写機2が設置されているエリアのセキュリティを管理する管理者が使用する管理者用情報処理端末などである。なお、出力照合判定部24による具体的な出力判定方法については後述する。

[0044] サーバ3から複写機2または通信端末26に警報情報を送信する方法には、特定の管理者宛てにメールで送るという方法もある。

[0045] [出力判定方法]

次に、図3乃至図5を参照して、サーバ3の出力照合判定部24による出力判定方法について説明する。

[0046] 出力判定データベース23は、上述のように、出力禁止情報または出力許可情報が登録されている。具体的には、出力判定データベース23には、出力禁止情報として、図3に示す禁止情報リスト、図4及び図5に示す出力制限テーブルなどが登録されている。

[0047] まず、出力照合判定部24が、図3に示すような禁止情報リストに基づいて出力を許可するか否か判定する場合について説明する。なお、複写機2からサーバ3が受信する情報は、複写情報読取部7が読み取ったイメージ情報又は当該イメージ情報をOCR(Optical Character Reader)等によりテキスト化したテキスト情報である。

[0048] 禁止情報リストは、図示のとおり、複写機2から受信した情報の出力を禁止する場合の条件をリスト化したものである。具体的に、出力照合判定部24は、複写機2から受信した情報が、「禁止文字を含む」、「個人名を10件以上含む」、「電話番号を10件以上含む」といった禁止情報リストに挙げられている1つ以上の条件と照合して一致した場合、出力を許可しないと判定し、複写機2または通信端末26に警報情報の送信又は出力動作を止める制御を行う。

[0049] ここで、禁止文字とは、例えば「社外秘」や「Confidential」といった文書に印刷された機密情報を示す記号や文字等が挙げられる。出力照合判定部24は、複写機2から受信したテキスト情報を検索して禁止文字が含まれていると判定した場合に、出力を許可しないと判定する。また、禁止文字は、黒ではなく赤などの目立つ色で着色されていることが多く、この場合、出力照合判定部24は、複写機2から受信したイメージ情報に基づいて着色された禁止文字が含まれていると判定した場合に、出力を許可しないと判定する。このように、禁止文字を含む情報の出力を禁止することで、サーバ3は、社外秘の情報を出力して持ち出した者を容易に特定することができる。

[0050] なお、禁止情報リストの条件は、図示されているものに限られず、任意に設定するこ

とができる。

[0051] また、個人名とはフルネームのことであり、サーバ3は、このような個人名や電話番号を10件以上含む情報を出力して持ち出した者を容易に特定することができる。つまり、個人情報漏洩を防止することができる。

[0052] 次に、出力照合判定部24が、図4に示すような社員の属性等に基づく出力制限テーブルを参照して出力を許可するか否かを判定する方法について説明する。社員の属性等に基づく出力制限テーブルは、図示のとおり、社員属性、出力可能時間帯、所属及び出力可能場所から構成されている。

[0053] 「社員属性」とは、正社員又はアルバイトのいずれか一方を示す情報であり、複写機2から受信したID情報及びID情報データベース14から特定することができる。出力可能時間帯とは、正社員又はアルバイトがそれぞれ情報を出力することができる時間帯であり、本実施形態では図示のように、正社員は「7:00ー0:00」と残業時間等を考慮して比較的長い時間出力することができ、アルバイトは「9:00ー17:00」と勤務時間内のみ出力することができる。なお、社員属性としては、他に社内の役職などを使用することもできる。「所属」とは、社員が属している部署を示す情報である。「出力可能場所」とは、社員が属している部署のフロアを示す情報であり、社員は、自己が所属する部署のフロアに設置された複写機2からのみ出力することができる。

[0054] 出力照合判定部24は、まず、複写機2から受信したID情報及びID情報データベース14から社員の属性及び所属を特定する。そして、出力照合判定部24は、当該属性に基づいて図4に示す出力制限テーブルを参照し、出力許可時間帯以外の時間帯である場合に、出力を許可しないと判定する。また、出力照合判定部24は、当該所属に基づいて図4に示す出力制限テーブルを参照し、出力可能場所以外に設置された複写機2である場合に、出力を許可しないと判定する。このように、出力制限テーブルに合致しない時間帯や複写機2である場合に出力を許可しないことで、サーバ3は、自分の勤務時間外に情報を出力した者や自分の所属する部署のフロア以外で情報を出力した者を容易に特定することができる。

[0055] 次に、出力照合判定部24が、図5に示すような複写機設置場所に基づく出力制限テーブルを参照して出力を許可するか否かを判定する場合について説明する。なお

、複写機2からサーバ3が受信する情報には、複写情報読取部7が読み取ったイメージ情報又はテキスト情報に加えて、当該複写機2を特定する情報、例えば後述するプリンタID等が含まれているものとする。また、複写機2は、ここではプリンタであるものとする。

[0056] 複写機設置場所に基づく出力制限テーブルは、図示のとおり、プリンタID、設置場所、社員IDから構成されている。「プリンタID」とは、プリンタを識別する情報である。「設置場所」とは、プリンタIDが示すプリンタの設置場所である。「社員ID」は、社員を識別する情報であり、複写機2から受信したID情報及びID情報データベース14から特定することができる。

[0057] 出力照合判定部24は、まず、複写機2から受信した情報に基づいて当該複写機2のプリンタIDを特定する。また、複写機2から受信したID情報及びID情報データベース14から社員IDを特定する。そして、出力照合判定部24は、特定したプリンタIDに基づいて図5に示す出力制限テーブルを参照し、対応する社員IDと特定した社員IDが一致しない場合に、出力を許可しないと判定する。このように、出力制限テーブルに合致しない社員IDの場合に出力を許可しないことで、サーバ3は、自分の所属する部署のフロア以外で情報を出力した者を容易に特定することができる。特に、フロア毎に異なる顧客の資料を取り扱うような場合、図示のような出力制限テーブルによって、正社員であっても自己が所属する部署のフロア以外で情報を出力させないようにすることは有益である。

[0058] [出力情報管理処理]

次に、図6及び図7を参照して、本発明の実施形態に係る出力情報管理システムによる処理手順及び出力情報管理方法について説明する。

[0059] まず、複写機2の利用者は、その利用者が持参したICカード1をカード情報読取部5のカード挿入口から挿入して、ICカード1の記憶部に記憶されているID情報をカード情報読取部5で読み取る(ステップS1)。次に、複写機2は、カード情報読取部5で読み取ったID情報を、通信部12で通信回線4を介してサーバ3に送信する(ステップS2)。ID情報を受信したサーバ3は、ID情報データベース14に登録されているID情報と、サーバ3で受信したID情報とについての照合処理を照合部16で行う(ステッ

プS3)。そして、照合部16による照合処理の結果において、照合が一致した場合には、サーバ3から複写機2に対して、複写機2による複写処理を許可する信号を送信し、複写機2の制御部13を複写可能な状態に制御させる(ステップS4)。また、照合部16による照合処理の結果において、照合が不一致である場合には、その後の処理を終了させる。この場合、サーバ3から複写機2に対して、照合処理が不一致であることを示す信号を、通信回線4を介して送信するようにしてもよい。

[0060] 次に、利用者は、複写したい原稿20を原稿セット部にセットして、複写情報読取部7により原稿内容を読み取る(ステップS5)。そして、複写情報読取部7で読み取られた原稿内容は、デジタル情報変換部8によりデジタル情報への変換処理が行われる(ステップS6)。また、複写部10により、複写用紙21上にその原稿内容が複写される(ステップS7)。この複写は、原稿内容が読み取られて後に直ぐに行っても良い。

[0061] 次に、その原稿内容からなるデジタル情報は、カード情報読取部5で読み取られたID情報と関係付けられた情報として、通信回線4を介してサーバ3に送信される(ステップS8)。このとき、複写機2(出力装置)が保持している機器識別情報や複写時間、複写場所などの情報を、ID情報と関連付けられた情報としてサーバ3に送信することで、より詳細な複写情報を登録することができる。次に、サーバ3は、複写機2から受信した、ID情報と、そのID情報に関係付けられた原稿内容からなるデジタル情報とを、出力情報データベース15に登録する(ステップS9)。出力情報データベース15には、ID情報と、そのID情報に関係付けられた原稿内容からなるデジタル情報とが時系列で順番に登録されていく。

[0062] 次に、サーバ3で受信した情報を、出力判定情報データベース23に登録されている情報と照合する(ステップS10)。照合の結果、出力判定情報データベース23に出力を禁止している情報であるか、または出力を不許可となっている情報である場合には、サーバ3から複写機2及び通信端末26に警報情報を送信する(ステップS11)。

[0063] 上記の処理により、出力情報データベース15に登録されたID情報に関係付けられた複写情報と、ID情報データベース14に登録されているID情報に関係付けられた個人情報とから、まず複写機2を使用した人を特定することができる。更に、誰が、どのような内容の複写を行ったのかについても、出力情報データベースにおいて、ID

情報に関係付けられて登録されている複写情報を調べることで、使用状況の詳細を簡単に調査することができる。

[0064] 尚、情報記憶媒体は、ICカードに限定されるものではなく、ID情報等の固有情報を記憶することができる記憶部を有する種々の情報記憶媒体であれば用いることができる。また、本発明は、複写機の他、情報を紙媒体に表示して出力する機能を有する各種の出力装置に適用することができる。また、出力装置である複写機2とサーバ3との間の情報の送受信において通信の安全性を高めるために、暗号システムを用いることが好ましい。

[0065] 例えば、情報記憶媒体であるICカードの記憶部に電子証明書を記憶させておく。処理の最初の段階で、ICカードの電子証明書を読み取った複写機2からサーバ3に対して電子証明書の送信を行った後に、サーバ3側で電子証明書の検証処理を行う。この検証処理での許可判定が出たことを条件に複写機2による複写処理を行えるようにする。

[0066] この処理により、その後における複写機2とサーバ3との間の通信を、SSL(Secure Socket Layer)を利用した通信で行うようにする。「SSL」とは、データの暗号化及び公開鍵暗号方式の電子証明書によるクライアント及び／又はサーバの認証を行うための仕組みである。このSSLでは、複写機2からサーバ3に対して、ID情報と、そのID情報に関係付けられた原稿内容からなるデジタル情報とを送信するのに先だって、電子証明書を付けて送信する。この際、電子証明書内の公開鍵と対になる秘密鍵を用いて、デジタル署名を行っても構わない。また、複写機2から送信する、ID情報と、そのID情報に関係付けられた原稿内容からなるデジタル情報とを、複数のサーバに分割して送信するようにしてもよい。これらの技術は、暗号化処理システム(特開2000—59355)に開示されている。複数のサーバで分割してこれらの情報を保管することで、データ保管のより高いセキュリティを確保することができるという利点がある。

第2実施形態

[0067] 図8乃至図11を参照して、本発明の第2実施形態について説明する。図8は、本発明の第2実施形態に係る出力情報管理システムの概要を説明するための図である。

図9は、本発明の第2実施形態に係る出力情報管理システムのシステムブロック図である。図10及び図11は、本発明の第2実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[0068] [出力情報管理システム]

まず、図8及び図9を参照して出力情報管理システムの概要について説明する。

[0069] 本発明の第2実施形態に係る出力情報管理システムは、図8に示すように、利用者用の情報記憶媒体であるICカード1と、ICカードリーダライタ42を備えたパソコンなどの情報処理端末43と、この情報処理端末43から情報の受信を可能に接続され、情報処理端末43から受信した情報を紙媒体に出力するプリンタなどの出力装置44と、出力装置44と通信回線45を介して通信可能に接続されているサーバ46とから構成されている。

[0070] 例えば、会社などの組織では、ビルのワンフロアーに複数の社員が個々のデスクにパソコンを置いて仕事をし、出力装置44は共通で使用するために1台や2台が所定の場所に設置される。各自が必要に応じて、自分のパソコンから複写機でプリントするための情報を送信して、紙媒体にプリント出力している。

[0071] 本発明においても、1台の出力装置44には、複数台のパソコンなどの情報処理端末43が情報を送信可能に接続されており、1台の出力装置44を複数の使用者が共通で使用して情報のプリント出力が行えるようにシステムが構成されている。また、サーバ46は、管理センターなどに設置して、通信回線45を介して複数の出力装置44と通信可能に接続され、共通して使用可能にシステム化されている。

[0072] ICカード1の記憶部には、ICカード1の使用者を特定することができるID情報と、プライベート鍵(秘密鍵)と、このプライベート鍵と対として用いる公開鍵を有する電子証明書とが記憶されている。また、出力装置44とサーバ46も、プライベート鍵と、電子証明書とをそれぞれ保持している。

[0073] そして、ICカードリーダライタ42は、ICカード1に記憶されている情報を読み取り情報処理端末43に送信する情報読取部47や、情報処理端末43からICカード1に情報を書き込む情報書込部48を有している。

[0074] また、図9に示すように、パソコンなどの情報処理端末43には、表示部49、送受信

部50、入力部51、記憶部52、暗号化部53、制御部54などが備えられている。

[0075] 出力装置44でプリント出力しようとする情報は、入力部51から入力した情報でもよいし、記憶部52に記憶させておいた情報でもよい。プリント出力しようとする情報は、セキュリティ保護のためにSSL方式で暗号化した状態で出力装置44へと送信される。

[0076] 情報処理端末43と出力装置44の間における情報の暗号化は、暗号化部53により、ICカード1と出力装置44とがそれぞれ持っている電子証明書を交換した上で認証して、セッション鍵(共通鍵)を共有し、その後の情報の暗号化はこのセッション鍵を用いて行う。

[0077] また、暗号化された情報を送るとき、使用者のICカード1内のプライベート鍵でデジタル署名を作成して、同時に送ってもかまわない。

[0078] また、出力装置44には、送受信部55、暗号化部56、復号部57、表示部58、操作部59、警報音発生部60、プリント出力部61、記憶部62、通信部63、制御部64などが備えられている。

[0079] 復号部57は、情報処理端末43から送信され、出力装置44で受信した暗号化された受信情報を復号する機能を有している。

[0080] プリント出力部61は、復号部57で復号された情報を紙媒体65にプリント出力する機能を有している。

[0081] 記憶部62には、出力装置44のプライベート鍵と、電子証明書とが記憶されている。尚、サーバ46の記憶部にもプライベート鍵と、電子証明書とが記憶されている。出力装置44からサーバ46へ情報を送る際にも、SSL方式で情報を暗号化する。ここで、出力装置44からサーバ46に送信する情報は、情報処理端末43から出力装置44に送信されて、プリント出力部61で紙媒体65にプリント出力された情報である。これら一連の処理は、記憶部62に記憶されている制御プログラムに基づいて処理される。

[0082] サーバ46には、通信部66、記憶部67、警報情報送信部68、出力照合判定部69、復号部70、登録部72、制御部73、ID情報データベース74、出力禁止情報データベース75、出力情報データベース76などが備えられている。

[0083] ID情報データベース74には、ICカード1に記憶されているID情報と、そのICカー

ド1の使用者を特定することができる情報として、例えば、社員番号、氏名、所属部署名、役職などが関係付けられて登録されている。

[0084] 出力禁止情報データベース75には、予め出力装置4からプリント出力することが禁止されている情報が登録されている。これらの出力禁止情報は、ID情報と関係付けられた人物の職務範囲や役職などによって、その人物毎に出力が禁止される場合と、出力してもよい場合とに分かれるようにすることもできる。

[0085] 出力情報データベース76は、出力装置44でプリント出力した情報と、そのプリント出力した人物が使用したICカード1に記憶されているID情報とを関係付けて、出力装置44の使用履歴情報を登録して随時蓄積する。したがって、出力情報データベース76とID情報データベース74に登録された情報から、誰が、どのような内容のプリント出力を行ったのかが調べられるようにしてある。

[0086] 登録部72は、出力装置44から送信されサーバ46で受信し、復号部70で復号したプリント出力情報と、同時に受信したID情報とを関係付けて出力情報データベース76に登録する機能を有している。

[0087] また、出力照合判定部69は、出力装置44から送信されサーバ46で受信したプリント出力情報が、出力禁止情報データベース75に登録されている出力禁止情報に該当する情報であるか否かを照合判定する機能を有している。なお、出力照合判定部69による具体的な出力判定方法については後述する。

[0088] そして、警報情報送信部68は、出力照合判定部69による判定の結果において、プリント出力が禁止されていると判定された際に、サーバ46から出力装置44に対して、出力装置44の警報音発生部60から警報音を発生させるための信号を送信する機能を有している。

[0089] 記憶部67には、制御プログラムが搭載され、制御部73による制御方法をコントロールしている。

[0090] [出力判定方法]

次に、サーバ46の出力照合判定部69による出力判定方法について説明する。

[0091] 第2実施形態において、出力装置44からサーバ46が受信する情報は、復号部70で復号したプリント出力情報であるが、当該情報は、イメージ情報又はテキスト情報で

ある。なお、図3乃至図5に示すような禁止情報リスト及び出力制限テーブルを、出力禁止情報データベース75に登録する場合は、上述の第1実施形態における出力判定方法と同様であるため、便宜上説明は省略する。

[0092] プリント出力情報がテキスト情報である場合、当該テキスト情報にデジタル署名が付与されていることがある。ここで、デジタル署名とは、オンライン上でやりとりされる電子文書について確かにその人本人が作成したものであるかどうかを確認する手段であり、紙文書の場合における押印に相当するものである。このデジタル署名に使用される公開鍵が誰のものかを保証するのが電子証明書であり、認証局と呼ばれる第三者機関が発行する。テキスト情報にこのようなデジタル署名が付与されている場合、当該デジタル署名を検証することで、当該テキスト情報を作成した者の所属や役職を特定することが可能である。

[0093] そこで、出力照合判定部69は、まず、出力装置44から受信したID情報及びID情報データベース74から利用者の所属や役職を特定する。また、出力照合判定部69は、出力装置44から受信したテキスト情報に付与されたデジタル署名を検証することで、当該テキスト情報を作成した者の所属や役職を特定する。そして、出力照合判定部69は、例えば、利用者の所属と署名者の所属とを照合し、一致しない場合に、出力を許可しないと判定することができる。また、出力照合判定部69は、例えば、利用者の役職と署名者の役職とを照合し、利用者の役職が署名者の役職よりも下位の場合に、出力を許可しないと判定することができる。このように、利用者及び署名者の権限に基づいて出力を許可するか否かを判定することで、サーバ46は、権限に違反して情報を出力した者や自分の所属する部署以外の情報を出力した者を容易に特定することができる。

[0094] [出力情報管理処理]

次に、本発明の第2実施形態に係る出力情報管理システムの処理手順を、図10及び図11に示すフローチャートに基づいて説明する。

[0095] まず、使用に際して、ICカードリーダライタ42にICカード1をセットし、ICカード1の記憶部に記憶されているID情報と電子証明書とをICカードリーダライタ42で読み取る(ステップS21)。ICカードリーダライタ42で読み取られたこれらの情報は、情報処

理端末43に送られる(ステップS22)。

[0096] 次に、情報処理端末43において、出力装置44でプリント出力する情報を特定した後に、この情報をSSL方式にて情報処理端末43と出力装置44で共有しているセッション鍵で暗号化して情報処理端末43から出力装置44に送信する(ステップS23、S24)。

[0097] 次に、出力装置44では、情報処理端末43から受信した情報を、情報処理端末43と出力装置44で共有しているセッション鍵で復号させる(ステップS25)。そして、復号させた情報をプリント出力部61により紙媒体65にプリント出力させる(ステップS26)。次に、紙媒体65にプリント出力させた情報を、SSL方式にて出力装置44とサーバ46で共有しているセッション鍵で暗号化してサーバ46へ送信させる(ステップS27、S28)。

[0098] サーバ46では、受信した情報を出力装置44とサーバ46で共有しているセッション鍵で復号させる(ステップS29)。復号させた情報は、出力禁止情報データベース75に登録されている出力禁止情報に該当しないか否かが照合判定される(ステップS30)。この照合判定の結果、出力禁止情報に該当すると判定された場合(ステップS30;NG)には、警告情報送信部68により、サーバ46から出力装置44に対して警報情報が送信される(ステップS31)。警報情報を受信した出力装置44では、警報音発生部60により警報音を発生させて、プリント出力が禁止されている情報がプリント出力されたことを知らせる(ステップS32)。

[0099] また、サーバ46においては、出力情報データベース76に、復号させた情報と、ICカードリーダライタ42から送られてきたID情報とを関係付けた状態で登録させる(ステップS33)。以上のようにして、出力装置44でプリント出力された情報は、全てID情報とを関係付けた状態で出力情報データベース76に登録され、プリント出力の履歴情報が蓄積される。

[0100] また、情報処理端末43から出力装置44に送信される情報や、出力装置44からサーバ46に送信される情報は、いずれもSSL方式により保護されているのでセキュリティが確保されている。

第3実施形態

[0101] 図12乃至図14を参照して、本発明の第3実施形態について説明する。図12は、本発明の第3実施形態に係る出力情報管理システムの概要を説明するための図である。図13は、本発明の第3実施形態に係る出力情報管理システムのシステムブロック図である。図14は、本発明の第3実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[0102] [出力情報管理システム]

まず、図12及び図13を参照して出力情報管理システムの概要について説明する。

[0103] 本発明の第3実施形態に係る出力情報管理システムは、図12に示すように、利用者用の情報記憶媒体であるICカード1と、ICカードリーダライタ42を備えたパソコンなどの情報処理端末43と、この情報処理端末43から情報の受信を可能に接続され、情報処理端末43から受信した情報の出力の可否を判定するサーバ46と、サーバ46と通信回線45を介して通信可能に接続されており、サーバ46を介して情報処理端末43から受信した情報を紙媒体に出力するプリンタなどの出力装置44とから構成されている。

[0104] なお、図12では、上述のように情報処理端末43とサーバ46とが専用線で接続されており、サーバ46と出力装置44とがインターネット等をはじめとする通信回線45を介して接続されている。しかし、本発明はこれに限定されるものではなく、図13に示すように、情報処理端末43、出力装置44及びサーバ46がそれぞれ通信回線45を介して相互に情報の授受が可能なように構成してもよい。

[0105] 例えば、会社などの組織では、ビルのワンフロアーに複数の社員が個々のデスクにパソコンを置いて仕事をし、出力装置44は共通で使用するために1台や2台が所定の場所に設置される。各自が必要に応じて、自分のパソコンから複写機でプリントするための情報を送信して、紙媒体にプリント出力している。

[0106] 本発明においても、1台の出力装置44には、複数台のパソコンなどの情報処理端末43が情報の送信可能に接続されており、1台の出力装置44を複数の使用者が共通で使用して情報のプリント出力が行えるようにシステムが構成されている。また、サーバ46は、管理センターなどに設置して、通信回線45を介して複数の出力装置44と通信可能に接続され、共通して使用可能にシステム化されている。

[0107] ICカード1の記憶部には、ICカード1の使用者を特定することができるID情報と、プライベート鍵と、このプライベート鍵と対として用いる公開鍵を有する電子証明書とが記憶されている。また、出力装置44とサーバ46も、プライベート鍵と、電子証明書とをそれぞれ保持している。

[0108] そして、ICカードリーダライタ42は、ICカード1に記憶されている情報を読み取り情報処理端末43に送信する情報読取部47や、情報処理端末43からICカード1に情報を書き込む情報書込部48を有している。

[0109] また、図13に示すように、パソコンなどの情報処理端末43には、表示部49、送受信部50、入力部51、記憶部52、暗号化部53、制御部54などが備えられている。

[0110] サーバ46を介して出力装置44でプリント出力しようとする情報は、入力部51から入力した情報でもよいし、記憶部52に記憶させておいた情報を用いてもよい。なお、プリント出力しようとする情報は、セキュリティ保護のためにSSL方式で暗号化した状態でサーバ46へと送信される。

[0111] 情報処理端末43とサーバ46の間における情報の暗号化は、暗号化部53により、ICカード1とサーバ46とがそれぞれ持っている電子証明書を交換した上で認証して、セッション鍵(共通鍵)を共有し、その後の情報の暗号化はこのセッション鍵を用いて行う。また、暗号化された情報を送るとき、使用者のICカード1内のプライベート鍵でデジタル署名を作成して、同時に送ってもかまわない。

[0112] サーバ46には、通信部66、記憶部67、警報情報送信部68、出力照合判定部69、復号部70、登録部72、制御部73、ID情報データベース74、出力禁止情報データベース75、出力情報データベース76、暗号化部77などが備えられている。

[0113] ID情報データベース74には、ICカード1に記憶されているID情報と、そのICカード1の使用者を特定することができる情報として、例えば、社員番号、氏名、所属部署名、役職などが関係付けられて登録されている。

[0114] 出力禁止情報データベース75には、予め出力装置44からプリント出力することが禁止されている情報が登録されている。これらの出力禁止情報は、ID情報と関係付けられた人物の職務範囲や役職などによって、その人物毎に出力が禁止される場合と、出力してもよい場合とに分かれるようにすることもできる。

[0115] 出力情報データベース76には、出力装置44でプリント出力する情報と、そのプリント出力した人物が使用したICカード1に記憶されているID情報とを関係付けて、出力装置44の使用履歴情報を登録して随時蓄積される。したがって、出力情報データベース76とID情報データベース74に登録された情報から、誰が、どのような内容のプリント出力を行ったのかが調べられるようにしてある。

[0116] 登録部72は、情報処理端末43から送信されサーバ46で受信し、復号部70で復号したプリント出力情報と、同時に受信したID情報とを関係付けて出力情報データベース76に登録する機能を有している。復号部70は、暗号化された受信情報を復号する機能を有しており、復号した情報がプリント出力情報及びID情報である。なお、プリント出力情報とは、利用者が出力装置44で出力しようとしている情報のことである。

[0117] また、出力照合判定部69は、情報処理端末43からサーバ46で受信したプリント出力情報が、出力禁止情報データベース75に登録されている出力禁止情報に該当する情報であるか否かを照合判定する機能を有している。出力照合判定部69が出力を許可すると判定した場合、サーバ46の通信部66は、プリント出力情報を出力装置44へ送信する。一方、出力照合判定部69が出力を許可しないと判定した場合、サーバ46の制御部73は、プリント出力情報を出力装置44へ送信しないよう制御する。なお、出力照合判定部69による具体的な出力判定方法については後述する。

[0118] そして、警報情報送信部68は、出力照合判定部69による判定の結果において、プリント出力が禁止されていると判定された際に、サーバ46から出力装置44に対して、出力装置44の警報音発生部60から警報音を発生させるための信号を送信する機能を有している。なお、警報音ではなく、プリント出力が禁止されている旨のメッセージを警報情報として送信することとしてもよい。

[0119] 記憶部67には、制御プログラムが搭載され、制御部73による制御方法をコントロールしている。また、記憶部67には、サーバ46のプライベート鍵と、電子証明書とが記憶されている。尚、出力装置44の記憶部にもプライベート鍵と、電子証明書とが記憶されている。サーバ46から出力装置44へ情報を送る際にも、SSL方式で情報を暗号化する。ここで、サーバ46から出力装置44に送信する情報としては、情報処理端

末43からサーバ46に送信されて、出力照合判定部69が出力を許可すると判定した場合に送信されるプリント出力情報である。これら一連の処理は、記憶部67に記憶されている制御プログラムに基づいて処理される。

[0120] 出力装置44には、送受信部55、暗号化部56、復号部57、表示部58、操作部59、警報音発生部60、プリント出力部61、記憶部62、通信部63、制御部64などが備えられている。

[0121] 復号部57は、サーバ46から送信され、出力装置44で受信した暗号化されたプリント出力情報を復号する機能を有している。

[0122] プリント出力部61は、復号部57で復号された情報を紙媒体65にプリント出力する機能を有している。

[0123] [出力判定方法]

サーバ46の出力照合判定部69による出力判定方法は、上述の第1実施形態及び第2実施形態における出力判定方法と同様であるため、便宜上説明は省略する。

[0124] なお、図5に示すような出力制限テーブルを参照して判定を行う場合、情報処理端末43からサーバ46が受信する情報には、情報を出力する予定の出力装置44を特定する情報、例えば出力装置44がプリンタである場合におけるプリンタID等が含まれているものとする。

[0125] [出力情報管理処理]

次に、本発明の第3実施形態に係る出力情報管理システムの処理手順を図14に示すフローチャートに基づいて説明する。

[0126] まず、使用に際して、ICカードリーダライタ42にICカード1をセットし、ICカード1の記憶部に記憶されているID情報と電子証明書とをICカードリーダライタ42で読み取る(ステップS41)。ICカードリーダライタ42で読み取られたこれらの情報は、情報処理端末43に送られる(ステップS42)。

[0127] 次に、情報処理端末43において、出力装置44でプリント出力する情報を特定した後に、この情報をSSL方式にて情報処理端末43とサーバ46で共有しているセッション鍵で暗号化して情報処理端末43からサーバ46に送信する(ステップS43、S44)。なお、情報処理端末43は、サーバ46との間のSSLで共有したセッション鍵で暗号化

を行う。

[0128] サーバ46では、情報処理端末43から受信した情報を、情報処理端末43とサーバ46で共有しているセッション鍵で復号させる。そして、復号させた情報は、出力禁止情報データベース75に登録されている出力禁止情報に該当しないか否かが判定される(ステップS45)。この照合判定部の結果、出力禁止情報に該当すると判定した場合(ステップS45;Yes)には、警報情報送信部68により、サーバ46から出力装置44に対して警報情報が送信される(ステップS46)。警報情報を受信した出力装置44では、警報音発生部60により警報音を発生させて、プリント出力が禁止されている情報であるためプリント出力できないことを知らせる。また、この場合、サーバ46は、情報処理端末43から受信した情報を出力装置44には送信しない。

[0129] 一方、照合判定部の結果、出力禁止情報に該当しないと判定した場合(ステップS45;No)には、サーバ46において、出力情報データベース76に、復号させた情報、即ちプリント出力情報と、ICカードリーダライタ42から送られてきたID情報とを関係付けた状態で登録させる(ステップS47)。このようにして、出力装置44で出力される情報は、全てID情報とを関係付けた状態で出力情報データベース76に登録され、プリント出力の履歴情報が蓄積される。また、サーバ46は、プリント出力情報をSSL方式にてサーバ46と出力装置44で共有しているセッション鍵で暗号化して出力装置44に送信する(ステップS48、S49)。なお、サーバ46は、出力装置44との間のSSLで共有したセッション鍵で暗号化を行う。このように、通信回線45を介して送受信される情報はいずれもSSL方式により保護されているのでセキュリティが確保されている。

[0130] 次に、出力装置44では、サーバ46から受信した情報を、サーバ46と出力装置44で共有しているセッション鍵で復号させる(ステップS50)。そして、復号させた情報をプリント出力部61により紙媒体65にプリント出力させる(ステップS51)。これにより、出力情報管理処理は完了する。

第4実施形態

[0131] 図15乃至図17を参照して、本発明の第4実施形態について説明する。図15は、本発明の第4実施形態に係る出力情報管理システムの概要を説明するための図である。図16は、本発明の第4実施形態に係る出力情報管理システムのシステムブロッ

ク図である。図17は、本発明の第4実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

[0132] [出力情報管理システム]

まず、図15及び図16を参照して出力情報管理システムの概要について説明する。

[0133] 本発明の第4実施形態に係る出力情報管理システムは、図15に示すように、利用者用の情報記憶媒体であるICカード1と、ICカードリーダライタ42を備えたパソコンなどの情報処理端末43と、この情報処理端末43から情報の受信を可能に接続され、情報処理端末43から受信した情報の出力の可否を判定する処理サーバ80と、処理サーバ80から情報の受信を可能に接続され、サーバ80を介して情報処理端末43から受信した情報を紙媒体に出力するプリンタなどの出力装置44とを構成要素として有している。また、出力情報管理システムは、処理サーバ80から情報の受信を可能に接続され、出力端末44がプリント出力した情報などを管理する保管サーバ81も構成要件として有している。

[0134] なお、図15では、上述のように情報処理端末43と処理サーバ80、処理サーバ80と出力装置44、処理サーバ80と保管サーバ81がそれぞれ専用線で接続されている。しかし、本発明はこれに限定されるものではなく、図15に示すように、情報処理端末43、出力装置44、処理サーバ80及び保管サーバ81がそれぞれ通信回線45を介して相互に情報の授受が可能なように構成してもよい。

[0135] 例えば、会社などの組織では、ビルのワンフロアーに複数の社員が個々のデスクにパソコンを置いて仕事をし、出力装置44は共通で使用するために1台や2台が所定の場所に設置される。各自が必要に応じて、自分のパソコンから複写機でプリントするための情報を送信して、紙媒体にプリント出力している。

[0136] 本実施形態においても、1台の出力装置44には、複数台のパソコンなどの情報処理端末43が情報の送信可能に接続されており、1台の出力装置44を複数の使用者が共通で使用して情報のプリント出力が行えるようにシステムが構成されている。また、処理サーバ80は集約させて1箇所に、保管サーバは例えばそれぞれのフロアに1箇所ずつ設置し、複数の情報処理端末43及び出力装置44が共通して使用可能にシステム化されているものとする。このように、処理サーバ80と保管サーバ81を分け

ることで、出力するプリンタ情報を判定する機能は処理サーバ3により1箇所で集約して行い、出力したプリンタ情報を履歴として記憶する機能はメモリ使用量が大きいため保管サーバにより複数箇所で行うことができる。

[0137] ICカード1の記憶部には、ICカード1の使用者を特定することができるID情報と、プライベート鍵と、このプライベート鍵と対として用いる公開鍵を有する電子証明書とが記憶されている。また、出力装置44、処理サーバ80及び保管サーバ81も、プライベート鍵と、電子証明書とをそれぞれ保持している。

[0138] そして、ICカードリーダライタ42は、ICカード1に記憶されている情報を読み取り情報処理端末43に送信する情報読取部47や、情報処理端末43からICカード1に情報を書き込む情報書込部48を有している。

[0139] また、図16に示すように、パソコンなどの情報処理端末43には、表示部49、送受信部50、入力部51、記憶部52、暗号化部53、制御部54などが備えられている。

[0140] サーバ46を介して出力装置44でプリント出力しようとする情報は、入力部51から入力した情報でもよいし、記憶部52に記憶させておいた情報を用いてもよい。なお、プリント出力しようとする情報は、セキュリティ保護のためにSSL方式で暗号化した状態で処理サーバ80へと送信される。

[0141] 情報処理端末43と処理サーバ80の間における情報の暗号化は、暗号化部53により、ICカード1と処理サーバ80とがそれぞれ持っている電子証明書を交換した上で認証して、セッション鍵(共通鍵)を共有し、その後の情報の暗号化はこのセッション鍵を用いて行う。また、暗号化された情報を送るとき、使用者のICカード1内のプライベート鍵でデジタル署名を作成して、同時に送ってもかまわない。

[0142] 処理サーバ80には、暗号化部84、記憶部85、通信部86、警報情報送信部87、出力照合判定部88、制御部89、復号部90、出力禁止情報データベース91、ID情報データベース92などが備えられている。

[0143] ID情報データベース92には、ICカード1に記憶されているID情報と、そのICカード1の使用者を特定することができる情報として、例えば、社員番号、氏名、所属部署名、役職などが関係付けられて登録されている。

[0144] 出力禁止情報データベース91には、予め出力装置44からプリント出力することが

禁止されている情報が登録されている。これらの出力禁止情報は、ID情報と関係付けられた人物の職務範囲や役職などによって、その人物毎に出力が禁止される場合と、出力してもよい場合とに分かれるようにすることもできる。

[0145] 出力照合判定部88は、情報処理端末43から処理サーバ80で受信したプリント出力情報が、出力禁止情報データベース91に登録されている出力禁止情報に該当する情報であるか否かを照合判定する機能を有している。出力照合判定部88が出力を許可すると判定した場合、処理サーバ80の通信部86は、プリント出力情報を出力装置44へ送信する。また、処理サーバ80の通信部86は、プリント出力情報及びID情報を保管サーバ81へ送信する。一方、出力照合判定部88が出力を許可しないと判定した場合、処理サーバ80の制御部89は、プリント出力情報を出力装置44へ送信しないよう制御する。なお、出力照合判定部88による具体的な出力判定方法については後述する。

[0146] 警報情報送信部87は、出力照合判定部88による判定の結果において、プリント出力が禁止されていると判定された際に、処理サーバ80から出力装置44に対して、出力装置44の警報音発生部60から警報音を発生させるための信号を送信する機能を有している。なお、警報音ではなく、プリント出力が禁止されている旨のメッセージを警報情報として送信することとしてもよい。

[0147] 記憶部85には、制御プログラムが搭載され、制御部89による制御方法をコントロールしている。また、記憶部85には、処理サーバ80のプライベート鍵と、電子証明書とが記憶されている。尚、出力装置44の記憶部や保管サーバ81の記憶部にもそれぞれプライベート鍵と、電子証明書とが記憶されている。

[0148] 処理サーバ80から出力装置44へ情報を送る際にも、SSL方式で情報を暗号化する。ここで、処理サーバ80から出力装置44に送信する情報としては、情報処理端末43から処理サーバ80に送信されて、出力照合判定部88が出力を許可すると判定した場合に送信されるプリント出力情報である。また、処理サーバ80から保管サーバ81へ情報を送る際にも、SSL方式で情報を暗号化する。ここで、処理サーバ80から保管サーバ81に送信する情報としては、出力照合判定部88が出力を許可すると判定した場合のプリント出力情報及び利用者のID情報である。これら一連の処理は、記

憶部85に記憶されている制御プログラムに基づいて処理される。

[0149] 保管サーバ81には、通信部93、記憶部94、復号部95、登録部96、制御部97、出力情報データベース98、ID情報データベース99などが備えられている。

[0150] ID情報データベース99には、上述と同様に、ICカード1に記憶されているID情報と、そのICカード1の使用者を特定することができる情報として、例えば、社員番号、氏名、所属部署名、役職などが関係付けられて登録されている。

[0151] 出力情報データベース98には、出力装置44でプリント出力する情報と、そのプリント出力した人物が使用したICカード1に記憶されているID情報とを関係付けて、出力装置44の使用履歴情報を登録して随時蓄積される。したがって、出力情報データベース97とID情報データベース99に登録された情報から、誰が、どのような内容のプリント出力を行ったのかが調べられるようにしてある。

[0152] 登録部96は、情報処理端末43から送信され処理サーバ80を介して保管サーバ81で受信し、復号部95で復号したプリント出力情報と、同時に受信したID情報とを関係付けて出力情報データベース98に登録する機能を有している。復号部95は、暗号化された受信情報を復号する機能を有しており、復号した情報がプリント出力情報及びID情報である。なお、プリント出力情報とは、利用者が出力装置44で出力しようとしている情報のことである。

[0153] 出力装置44には、送受信部55、暗号化部56、復号部57、表示部58、操作部59、警報音発生部60、プリント出力部61、記憶部62、通信部63、制御部64などが備えられている。

[0154] 復号部57は、処理サーバ80から送信され、出力装置44で受信した暗号化されたプリント出力情報を復号する機能を有している。

[0155] プリント出力部61は、復号部57で復号された情報を紙媒体65にプリント出力する機能を有している。

[0156] [出力判定方法]

処理サーバ80の出力照合判定部88による出力判定方法は、上述の第1実施形態及び第2実施形態における出力判定方法と同様であるため、便宜上説明は省略する。

[0157] [出力情報管理処理]

次に、本発明の第4実施形態に係る出力情報管理システムの処理手順を図17に示すフローチャートに基づいて説明する。

[0158] まず、使用に際して、ICカードリーダライタ42にICカード1をセットし、ICカード1の記憶部に記憶されているID情報と電子証明書とをICカードリーダライタ42で読み取る(ステップS61)。ICカードリーダライタ42で読み取られたこれらの情報は、情報処理端末43に送られる(ステップS62)。

[0159] 次に、情報処理端末43において、出力装置44でプリント出力する情報を特定した後に、この情報をSSL方式にて情報処理端末43と処理サーバ80で共有しているセッション鍵で暗号化して情報処理端末43から処理サーバ80に送信する(ステップS63、S64)。なお、情報処理端末43は、処理サーバ80との間のSSLで共有したセッション鍵で暗号化を行う。

[0160] 処理サーバ80では、情報処理端末43から受信した情報を、情報処理端末43と処理サーバ80で共有しているセッション鍵で復号させる(ステップS65)。そして、復号させた情報は、出力禁止情報データベース91に登録されている出力禁止情報に該当しないか否かが判定される(ステップS66)。この照合判定部の結果、出力禁止情報に該当すると判定した場合(ステップS66;Yes)には、警報情報送信部87により、処理サーバ80から出力装置44に対して警報情報が送信される(ステップS67)。警報情報を受信した出力装置44では、警報音発生部60により警報音を発生させて、プリント出力が禁止されている情報であるためプリント出力できないことを知らせる。また、この場合、処理サーバ80は、情報処理端末43から受信した情報を出力装置44に送信しない。

[0161] 一方、照合判定部の結果、出力禁止情報に該当しないと判定した場合(ステップS66;No)、処理サーバ80の暗号化部84は、復号させた情報、即ちプリント出力情報と、ICカードリーダライタ42から送られてきたID情報とを、保管サーバ81との間のSSLで共有したセッション鍵で暗号化する(ステップS68)。そして、処理サーバ80の通信部86は、暗号化したプリント出力情報及びID情報を、通信回線45を介して、保管サーバ81へ送信する(ステップS69)。保管サーバ81では、復号部95により処理サ

ーバ80から受信した情報を、処理サーバ80と保管サーバ81で共有しているセッション鍵で復号させる(ステップS70)。そして、保管サーバ81の登録部96は、出力情報データベース98に復号させたプリント出力情報及びID情報を関係付けた状態で登録させる(ステップS71)。

[0162] また、照合判定部の結果、出力禁止情報に該当しないと判定した場合(ステップS67;Yes)、処理サーバ80の暗号化部84は、復号させたプリント出力情報を、出力装置44との間のSSLで共有したセッション鍵で暗号化する(ステップS72)。そして、処理サーバ80の通信部86は、暗号化したプリント出力情報を出力装置44へ送信する(ステップS73)。このように、通信回線45を介して送受信される情報はいずれもSSL方式により保護されているので、セキュリティが確保されている。

[0163] 次に、出力装置44では、処理サーバ80から受信した情報を、処理サーバ80と出力装置44で共有しているセッション鍵で復号させる(ステップS74)。そして、復号させた情報をプリント出力部61により紙媒体65にプリント出力させる(ステップS75)。これにより、出力情報管理処理は完了する。

[0164] [変形例]

なお、上記第3及び第4実施形態では、サーバ46や処理サーバ80が出力を許可したプリンタ出力情報をID情報と関係付けて出力情報データベースに記憶することとしているが、本発明はこれに限定されるものではなく、情報処理端末43から受信した全てのプリンタ出力情報をID情報と関係付けて記憶することとしてもよい。これによれば、現実に出力装置44により出力されていないプリンタ出力情報も記憶されることとなるが、不正な出力を行おうとした利用者を記憶しておくことができる。

[0165] なお、上記第1乃至第4実施形態では、利用者のID情報を記憶している情報記憶媒体としてICカードを例に説明しているが、本発明はこれに限定されるものではなく、利用者の個人情報を記憶することができるものであれば種々のものを適用することができる。例えば、利用者の個人情報が記憶された情報記憶媒体を有する携帯電話やPDA(Personal Digital Assistant)を適用することができる。

[0166] また、上記第1乃至第4実施形態では、ICカードリーダライタ42によりICカードに記憶されているID情報を取得することとしているが、本発明はこれに限定されるもので

はなく、Bluetooth(登録商標)等を利用した無線通信により所定の情報記憶媒体に記憶されているID情報を取得することとしてもよい。即ち、本発明における情報記憶媒体とは、利用者の情報を記憶することができる媒体及び当該媒体を有する端末を含む概念であるものとする。

産業上の利用可能性

[0167] 本発明に係る出力情報管理システムは、情報を出力する装置が設置されている会社や役所などで広範囲に利用することができる。

請求の範囲

[1] 利用者用の情報記憶媒体と、媒体に情報を出力する出力装置と、前記出力装置と通信回線を介して通信可能に接続されているサーバとを備える出力情報管理システムであって、

前記情報記憶媒体は、固有情報が記憶された記憶部を有し、

前記出力装置は、前記情報記憶媒体から固有情報を読み取る読取部と、媒体に出力する情報を前記読取部で読み取った固有情報と関係付けた情報として前記サーバに送信する手段と、を有し、

前記サーバは、前記出力装置から受信した固有情報と関係付けられた情報を記憶させておくデータベースを有することを特徴とする出力情報管理システム。

[2] 前記サーバは、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されたデータベースと、

前記出力装置から受信した情報を前記データベースに登録されている情報と照合する照合部と、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置または管理者用情報処理端末に警報情報を送信する手段あるいは出力動作を止める手段を備えていることを特徴とする請求項1に記載の出力情報管理システム。

[3] 前記データベースは、前記出力装置毎に前記出力禁止情報、または前記出力許可情報が登録されており、

前記照合部は、前記出力装置から受信した情報を、当該出力装置に対応する前記出力禁止情報、または当該出力装置に対応する前記出力許可情報と照合することを特徴とする請求項2に記載の出力情報管理システム。

[4] 利用者が所持する情報記憶媒体と、媒体に情報を出力する出力装置と、前記出力装置と通信回線を介して通信可能に接続されているサーバとを備える出力情報管理システムにおける出力情報管理方法であって、

前記出力装置が、前記情報記憶媒体の記憶部に記憶された固有情報を読み取る

ステップと、

前記出力装置から前記サーバに、前記出力装置で出力した情報を前記固有情報と関連付けた情報として送信するステップと、

前記サーバで受信した前記固有情報と関連付けられた情報を、前記サーバのデータベースに記憶させるステップと、を有することを特徴とする出力情報管理方法。

[5] 情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを有する情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、前記出力装置と通信可能に接続されているサーバと、を備える出力情報管理システムであって、

前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、

前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、

前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記出力装置に送信する手段とを有し、

前記出力装置は、前記情報処理端末から受信したID情報と出力情報とを前記サーバに送信する手段を有し、

前記サーバは、前記前記出力装置から受信したID情報と出力情報とを関係付けてデータベースに記憶させる手段を有することを特徴とする出力情報管理システム。

[6] 情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを有する情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記出力装置と通信可能に接続されているサーバと、前記サーバを介して前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、を備える出力情報管理システムであって、

前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、

前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、

前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記サーバに送信する手段とを有し、

前記サーバは、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、

前記情報処理端末から受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、

前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信する出力情報送信部と、を有することを特徴とする出力情報管理システム。

[7] サーバは、

前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、

前記情報処理端末から受信したID情報と、前記照合部による照合の結果、前記出力禁止情報と不一致となった出力情報、または前記出力許可情報と一致した出力情報とを関係付けて出力情報データベースに記憶させる手段と、をさらに有することを特徴とする請求項6に記載の出力情報管理システム。

[8] 情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを有する情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記出力装置と通信可能に接続されている処理サーバと、前記処理サーバが出力を許可した情報を記憶する保管サーバと、前記処理サーバを介して前記情報処理端末から受信した情報を紙媒体に出力する出力装置とを備える出力情報管理システムであって、

前記情報記憶媒体は、利用者を特定可能なID情報が記憶された記憶部を有し、

前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取部を有し、

前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で

紙媒体に出力する出力情報とを前記処理サーバに送信する手段とを有し、

前記処理サーバは、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、

前記情報処理端末から受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、

前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信し、前記出力情報及びID情報を前記保管サーバに送信する送信部とを有し、

前記保管サーバは、

前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、

前記処理サーバから受信したID情報と出力情報とを関係付けて前記出力情報データベースに記憶させる手段と、をさらに有することを特徴とする出力情報管理システム。

[9] 前記出力判定情報データベースは、前記出力装置毎に前記出力禁止情報、または前記出力許可情報が登録されており、

前記照合部は、前記情報処理端末から受信した情報を、出力を予定している出力装置に対応する前記出力禁止情報、または当該出力装置に対応する前記出力許可情報と照合することを特徴とする請求項6乃至8のいずれか一項に記載の出力情報管理システム。

[10] 前記情報記憶媒体が、ICカードであることを特徴とする請求項5乃至9のいずれか一項に記載の出力情報管理システム。

[11] 媒体に情報を出力する出力装置と通信回線を介して接続されているサーバであって、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されたデータベースと、

前記出力装置から、前記媒体に出力する出力情報と、前記利用者の固有情報とを受信する受信部と、

前記出力装置から受信した出力情報と固有情報とを関係付けてデータベースに記憶する記憶部と、

前記出力装置から受信した出力情報を、前記データベースに登録されている情報と照合する照合部と、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置または管理者用情報処理端末に警報情報を送信する手段あるいは出力動作を止める手段とを有することを特徴とするサーバ。

[12] 情報を紙媒体に出力する出力装置と通信可能に接続されているサーバであって、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、

前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、

利用者を特定可能なID情報と、前記紙媒体に出力する出力情報とを受信する受信部と、

前記受信部が受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部と、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部と、

前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信する出力情報送信部と、

前記受信部が受信したID情報と、前記照合部による照合の結果、前記出力禁止

情報と不一致となった出力情報、または前記出力許可情報と一致した出力情報とを関係付けて出力情報データベースに記憶させる手段とを有することを特徴とするサーバ。

[13] 媒体に情報を出力する出力装置と通信回線を介して接続されているコンピュータにより実行されるプログラムであって、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されたデータベースを有しており、

前記出力装置から、前記媒体に出力する出力情報と、前記利用者の固有情報とを受信する受信部、

前記出力装置から受信した出力情報と固有情報とを関係付けてデータベースに記憶する記憶部、

前記出力装置から受信した出力情報を、前記データベースに登録されている情報と照合する照合部、

前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出力許可情報と不一致となった場合に、前記出力装置または管理者用情報処理端末に警報情報を送信する手段あるいは出力動作を止める手段として前記コンピュータを機能させることを特徴とするプログラム。

[14] 情報を紙媒体に出力する出力装置と通信可能に接続されているコンピュータにより実行されるプログラムであって、

前記出力装置で出力を禁止している出力禁止情報、または前記出力装置で出力を許可している出力許可情報が登録されている出力判定情報データベースと、

前記情報処理端末から受信したID情報と、出力情報とを関係付けて記憶している出力情報データベースと、を有しており、

利用者を特定可能なID情報と、前記紙媒体に出力する出力情報とを受信する受信部、

前記受信部が受信した出力情報を、前記出力判定情報データベースに登録されている情報と照合する照合部、

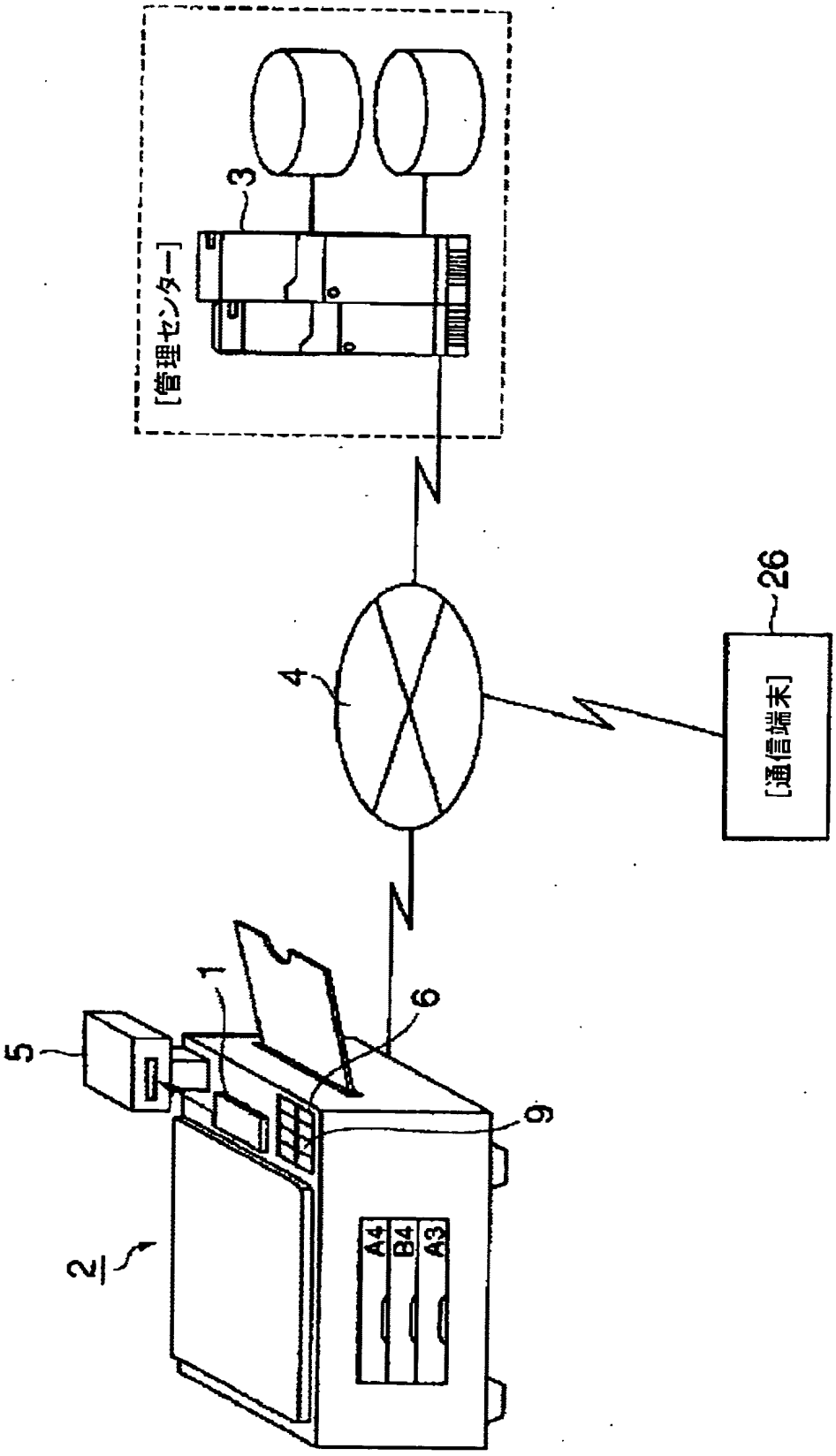
前記照合部による照合の結果、前記出力禁止情報と一致した場合、または前記出

力許可情報と不一致となった場合に、前記出力装置に警報情報を送信する警報情報送信部、

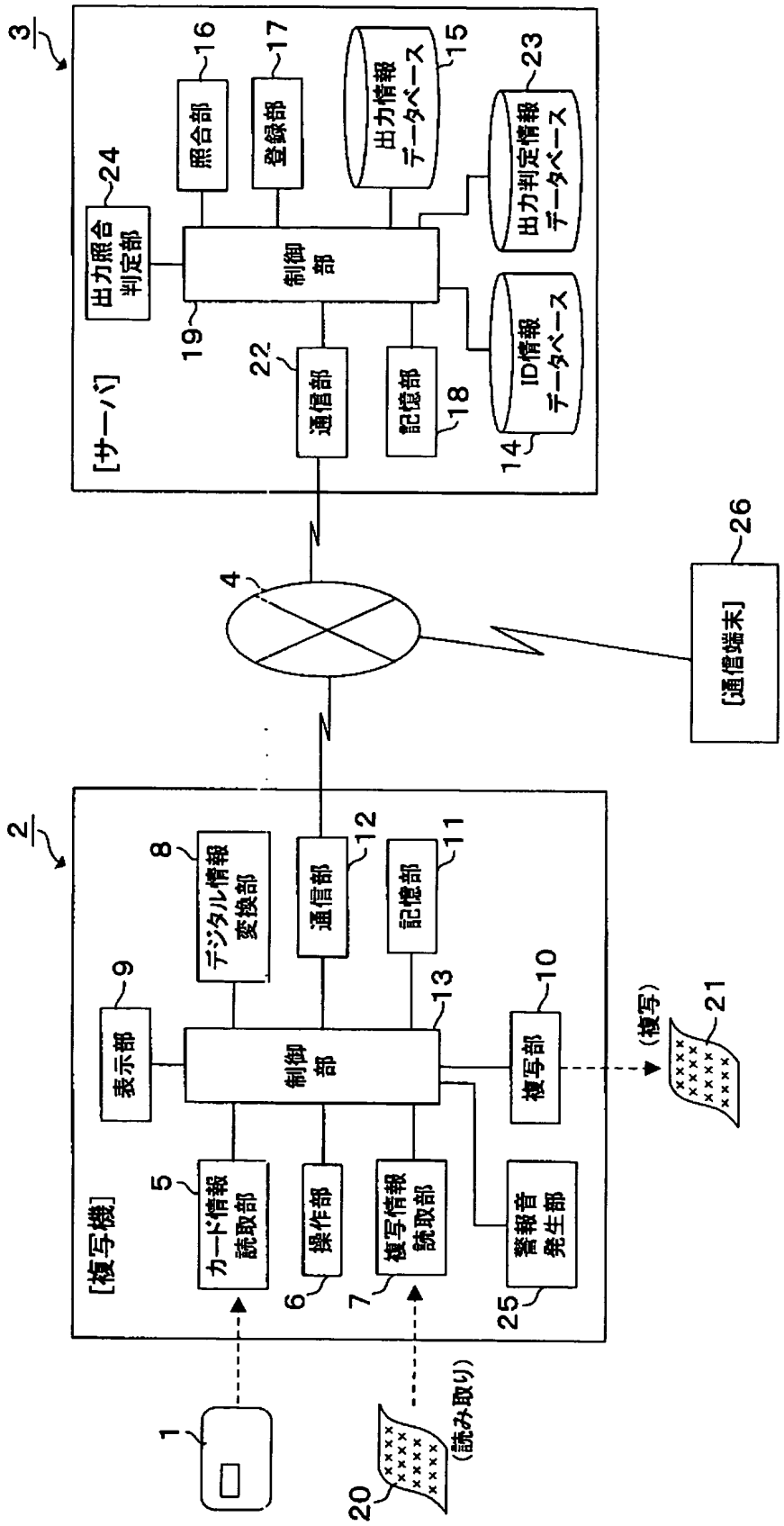
前記照合部による照合の結果、前記出力禁止情報と不一致となった場合、または前記出力許可情報と一致した場合に、前記出力情報を前記出力装置に送信する出力情報送信部、

前記受信部が受信したID情報と、前記照合部による照合の結果、前記出力禁止情報と不一致となった出力情報、または前記出力許可情報と一致した出力情報とを関係付けて出力情報データベースに記憶させる手段として前記コンピュータを機能させることを特徴とするプログラム。

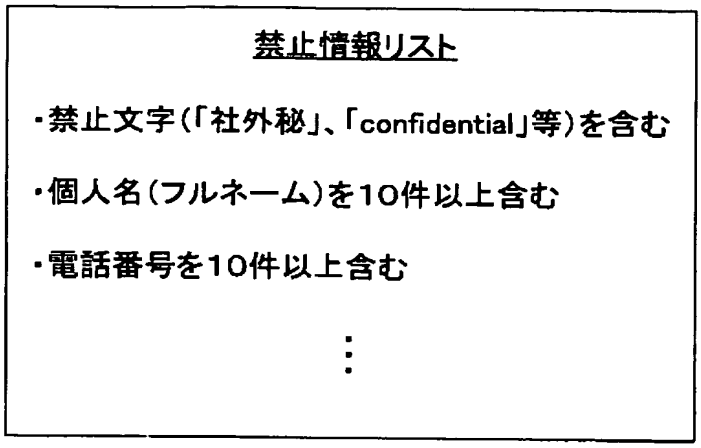
[図1]



[図2]


3
[サーバ]
16
照合部
17
登録部
15
出力情報データベース
23
出力判定情報データベース
24
出力照合判定部
制御部
19
22
通信部
18
記憶部
14
ID情報データベース
4
26
[通信端末]
2
[複写機]
8
デジタル情報変換部
12
通信部
11
記憶部
9
表示部
制御部
13
10
複写部
(複写)
21
5
カード情報読取部
操作部
6
複写情報読取部
7
警報音発生部
25
1
(読み取り)
20

[図3]



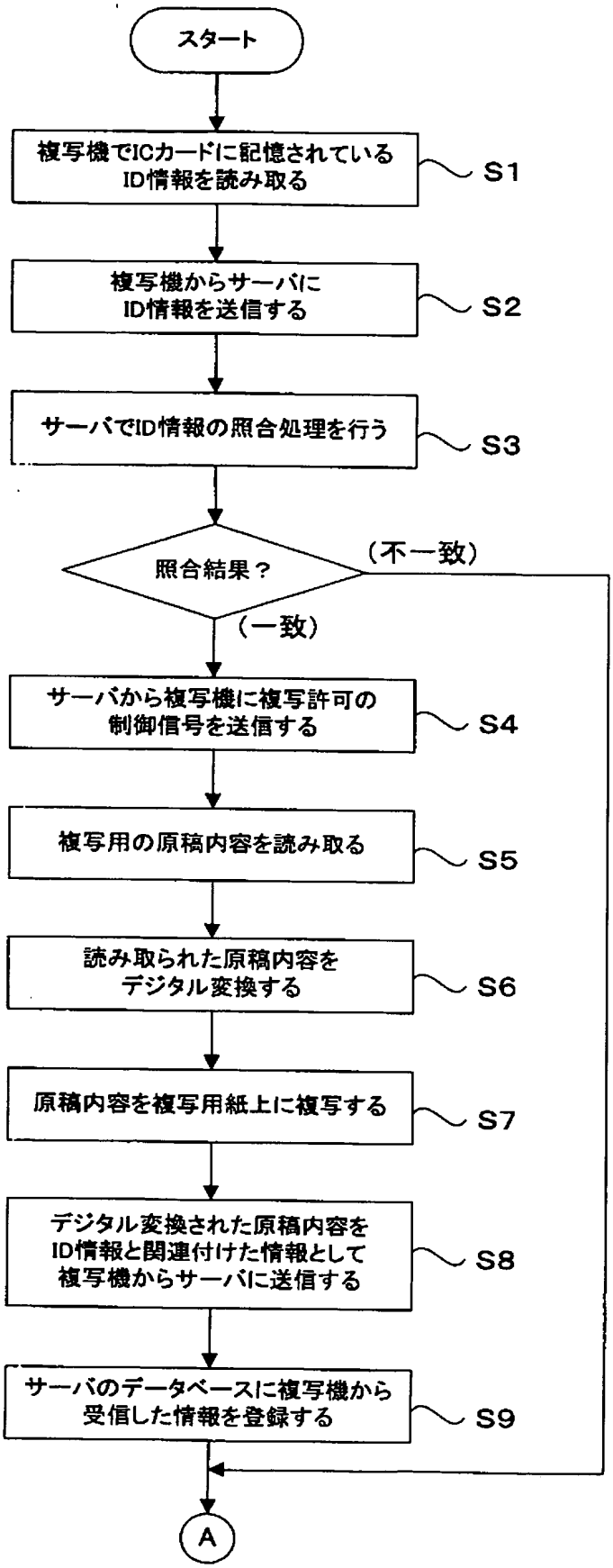
[図4]

社員属性	出力可能時間帯	所属	出力可能場所
正社員	7:00～0:00	総務部	フロアA
		人事部	フロアB
		開発部	フロアC
		⋮	⋮
アルバイト	9:00～17:00	総務部	フロアA
		人事部	フロアB
		開発部	フロアC
		⋮	⋮

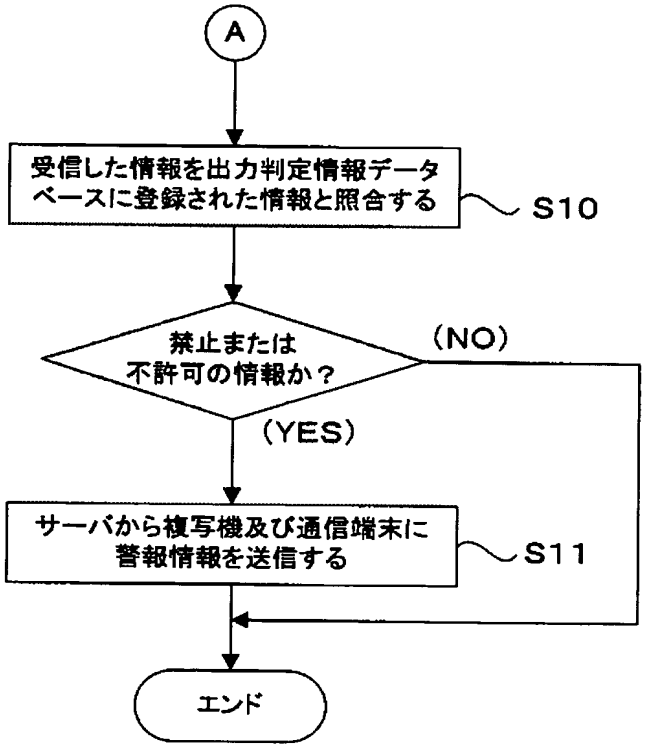
[図5]

プリンタID	設置場所	社員ID
プリンタA	A社開発フロア	P001～P100
プリンタB	B社開発フロア	P101～P200
プリンタC	C社開発フロア	P201～P300
⋮	⋮	⋮

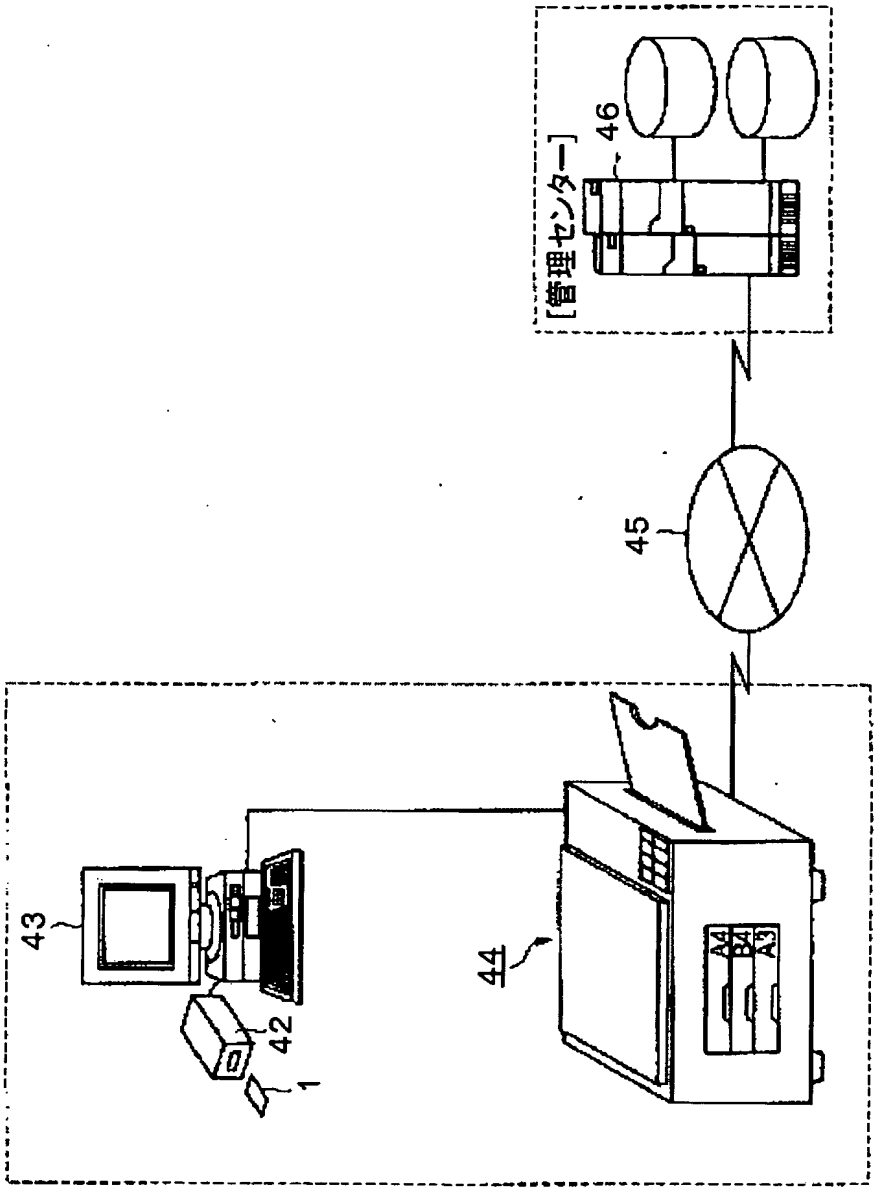
[図6]


スタート
複写機でICカードに記憶されている
ID情報を読み取る
S1
複写機からサーバに
ID情報を送信する
S2
サーバでID情報の照合処理を行う
S3
照合結果？
(不一致)
(一致)
サーバから複写機に複写許可の
制御信号を送信する
S4
複写用の原稿内容を読み取る
S5
読み取られた原稿内容を
デジタル変換する
S6
原稿内容を複写用紙上に複写する
S7
デジタル変換された原稿内容を
ID情報と関連付けた情報として
複写機からサーバに送信する
S8
サーバのデータベースに複写機から
受信した情報を登録する
S9
A

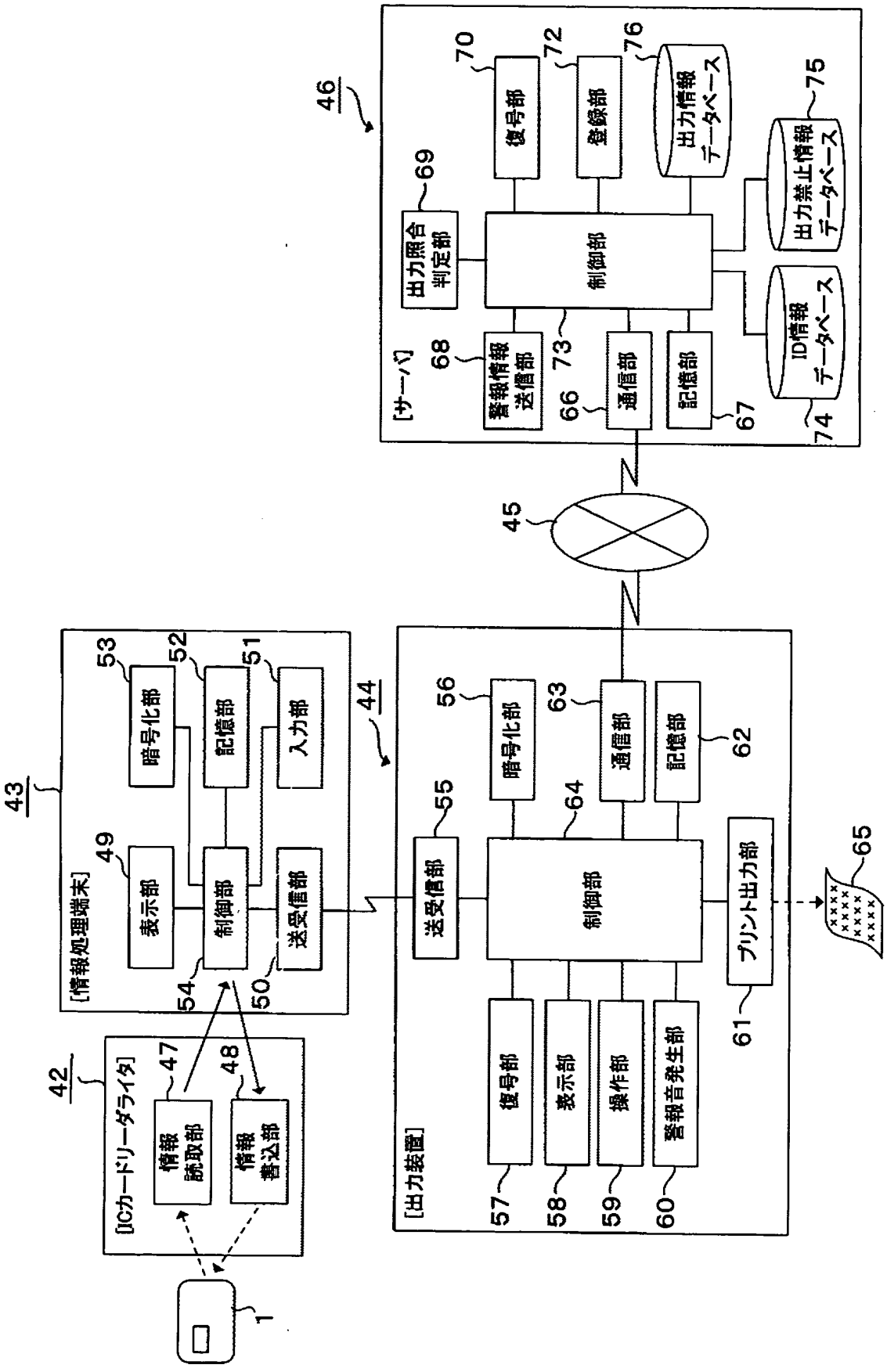
[図7]


A
受信した情報を出力判定情報データベースに登録された情報と照合する
S10
禁止または不許可の情報か？
(NO)
(YES)
サーバから複写機及び通信端末に警報情報を送信する
S11
エンド

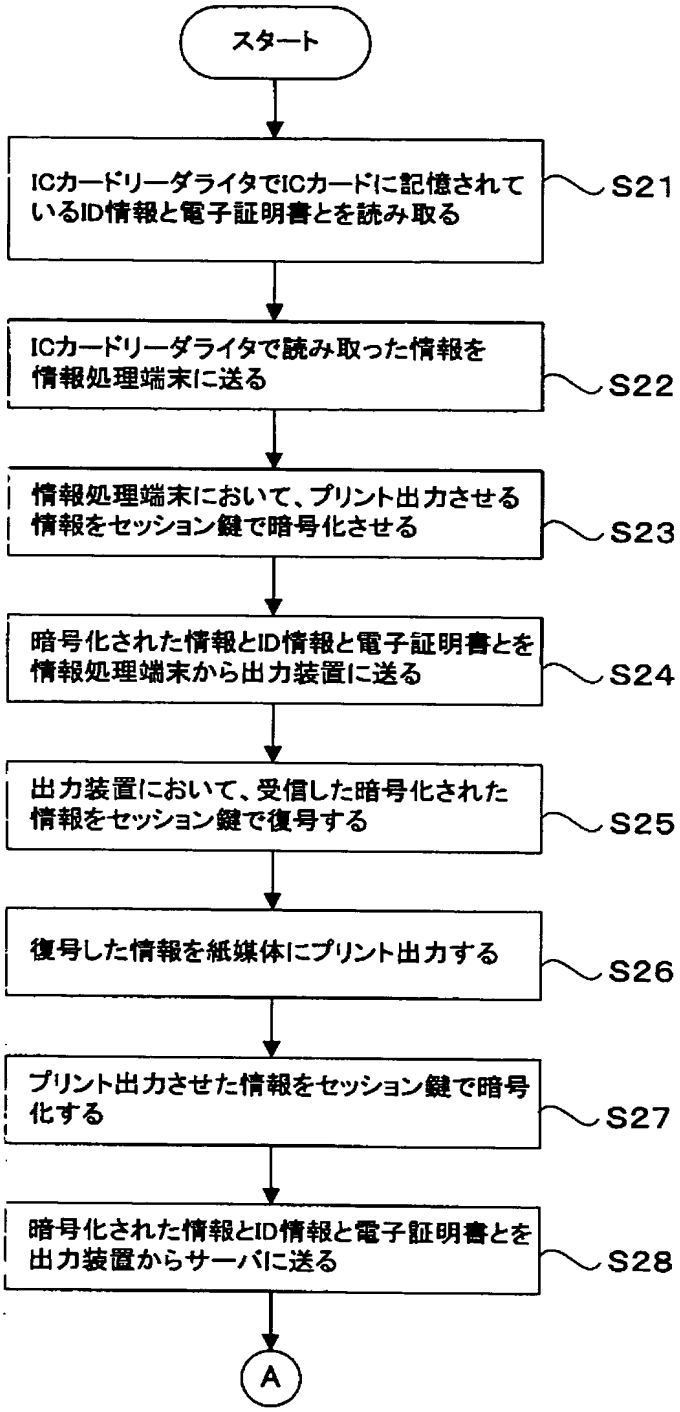
[図8]



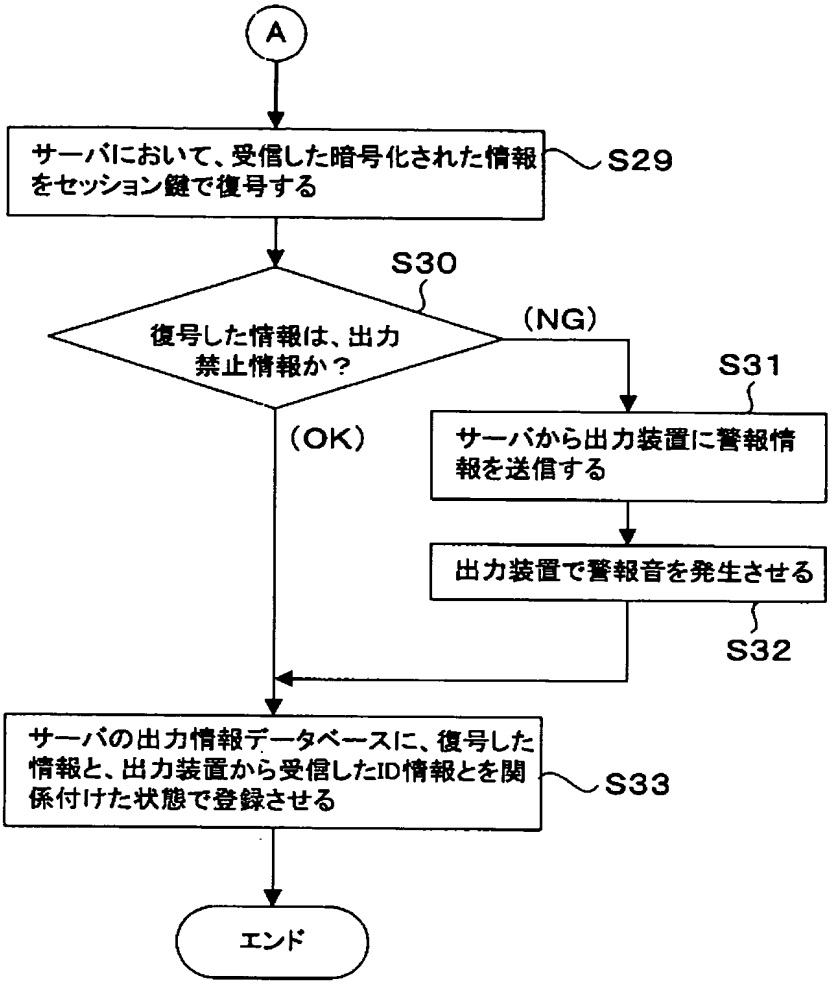
[図9]


46
[サーバ]
70
復号部
72
登録部
76
出力情報データベース
75
出力禁止情報データベース
69
出力照合判定部
制御部
68
警報情報送信部
73
66
通信部
67
記憶部
74
ID情報データベース
45
43
[情報処理端末]
53
暗号化部
52
記憶部
51
入力部
49
表示部
制御部
送受信部
54
50
44
[出力装置]
56
暗号化部
63
通信部
62
記憶部
55
送受信部
64
制御部
プリント出力部
65
61
復号部
57
表示部
58
操作部
59
警報音発生部
60
42
[ICカードリーダライタ]
47
情報読取部
48
情報書込部
1

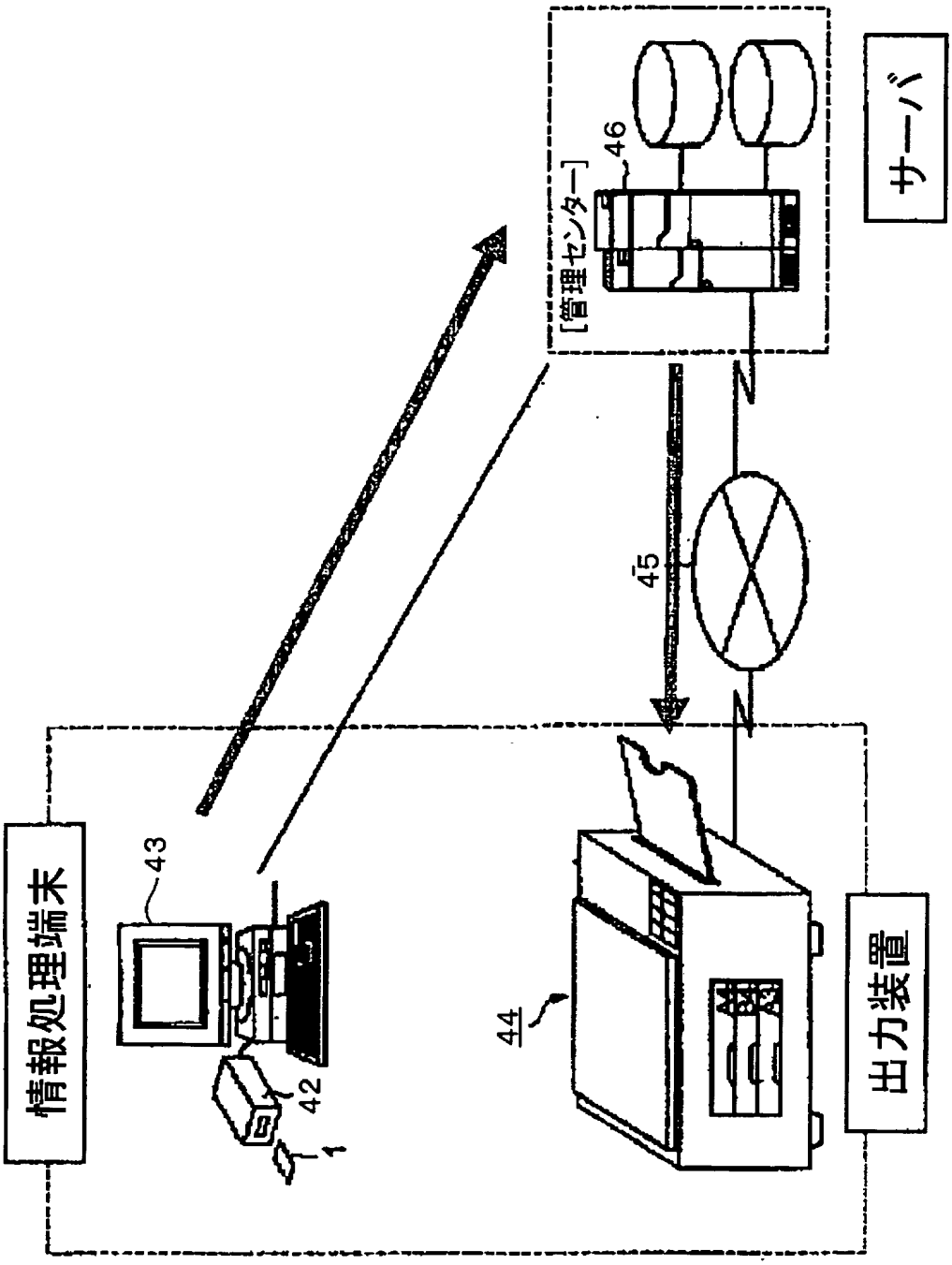
[図10]


スタート
ICカードリーダライタでICカードに記憶されているID情報と電子証明書とを読み取る
S21
ICカードリーダライタで読み取った情報を情報処理端末に送る
S22
情報処理端末において、プリント出力させる情報をセッション鍵で暗号化させる
S23
暗号化された情報とID情報と電子証明書とを情報処理端末から出力装置に送る
S24
出力装置において、受信した暗号化された情報をセッション鍵で復号する
S25
復号した情報を紙媒体にプリント出力する
S26
プリント出力させた情報をセッション鍵で暗号化する
S27
暗号化された情報とID情報と電子証明書とを出力装置からサーバに送る
S28
A

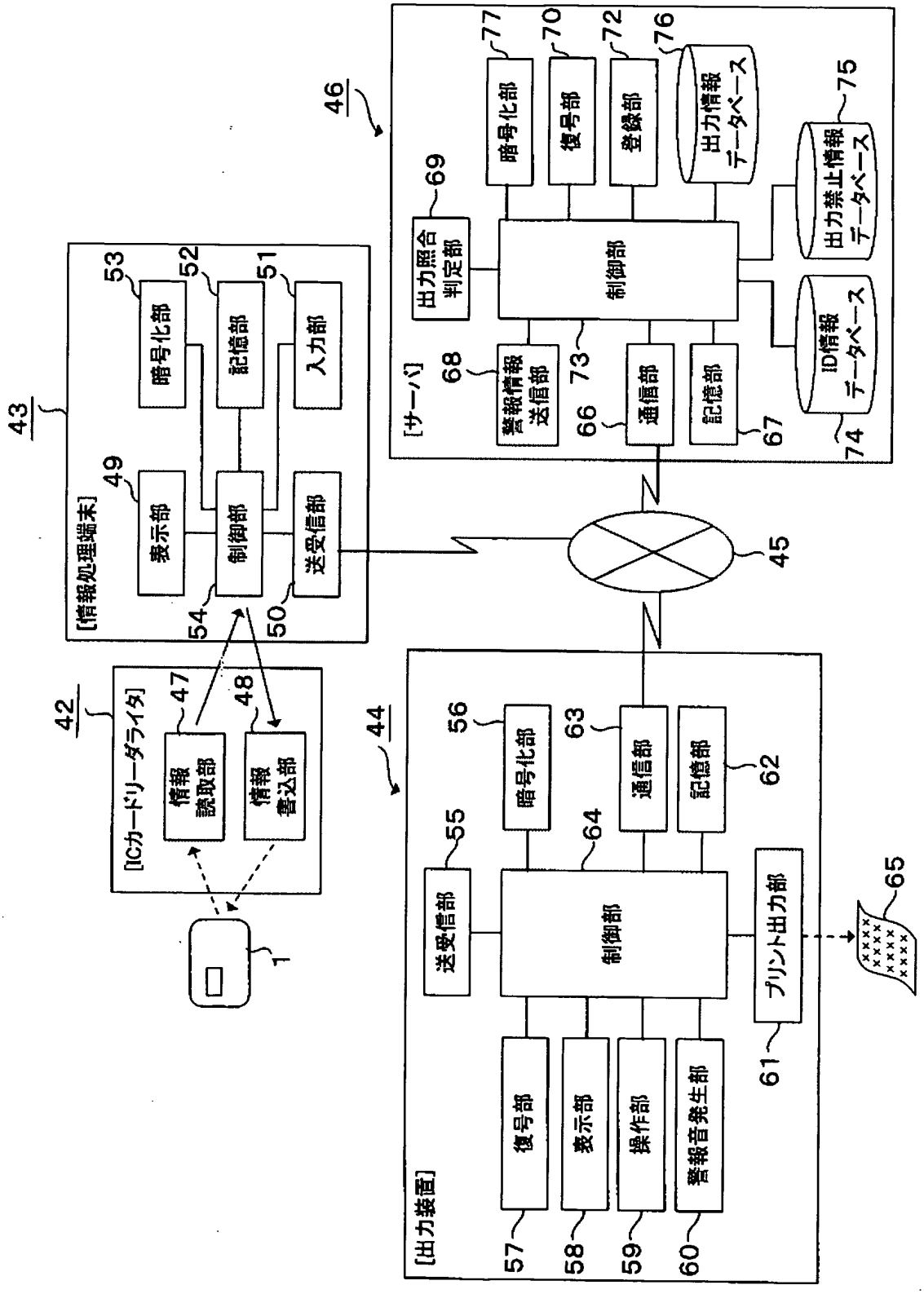
[図11]


A
サーバにおいて、受信した暗号化された情報をセッション鍵で復号する
S29
S30
復号した情報は、出力禁止情報か？
(NG)
(OK)
S31
サーバから出力装置に警報情報を送信する
出力装置で警報音を発生させる
S32
サーバの出力情報データベースに、復号した情報と、出力装置から受信したID情報とを関係付けた状態で登録させる
S33
エンド

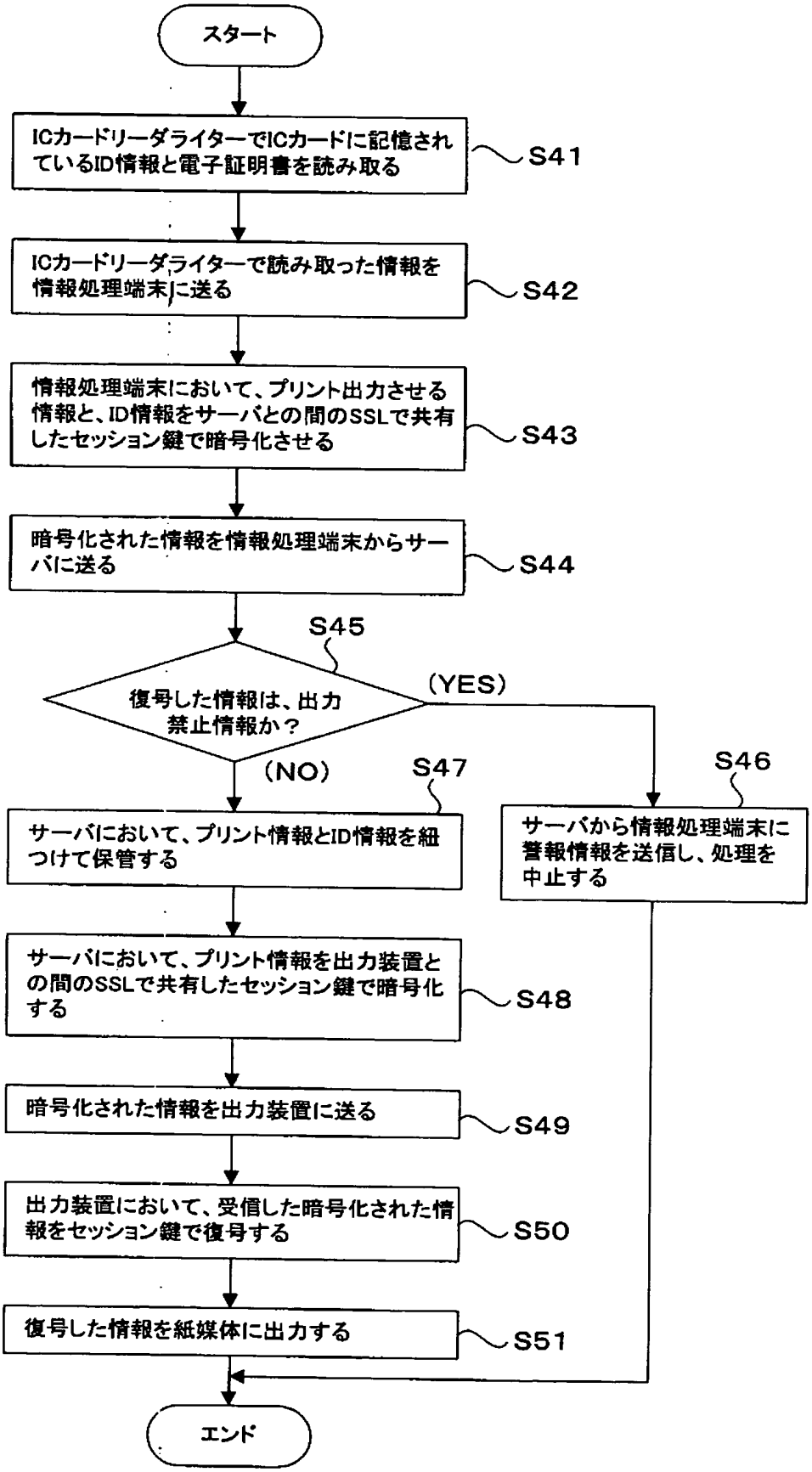
[図12]



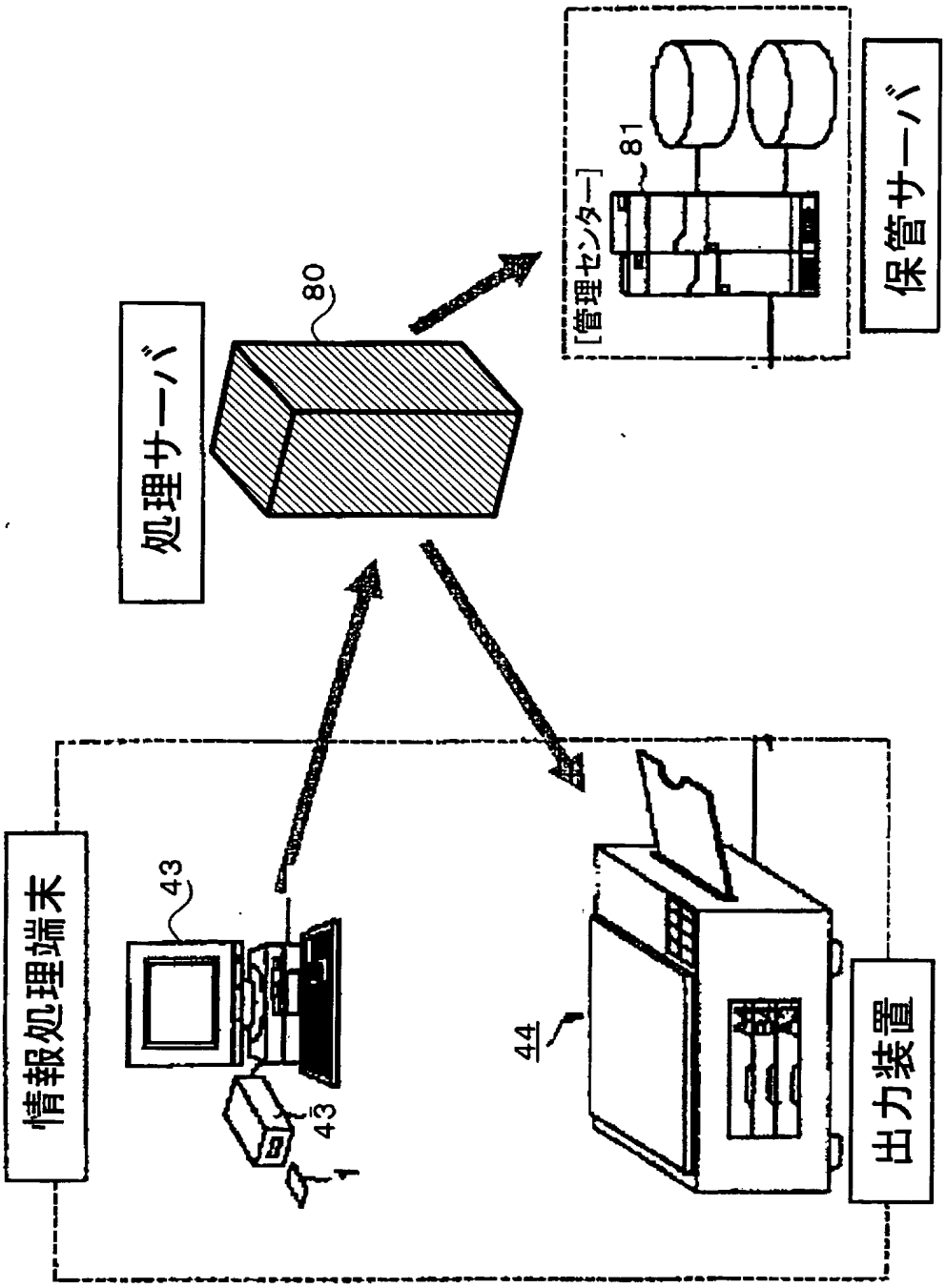
[図13]


[情報処理端末]
43
暗号化部
53
記憶部
52
入力部
51
表示部
49
制御部
54
送受信部
50
[ICカードリーダライタ]
42
情報読取部
47
情報書込部
48
1
45
[サーバ]
46
出力照合判定部
69
暗号化部
77
復号部
70
登録部
72
出力情報データベース
76
出力禁止情報データベース
75
制御部
警報情報送信部
68
通信部
66
記憶部
67
ID情報データベース
74
[出力装置]
44
送受信部
55
暗号化部
56
制御部
64
通信部
63
記憶部
62
プリント出力部
61
65
復号部
57
表示部
58
操作部
59
警報音発生部
60

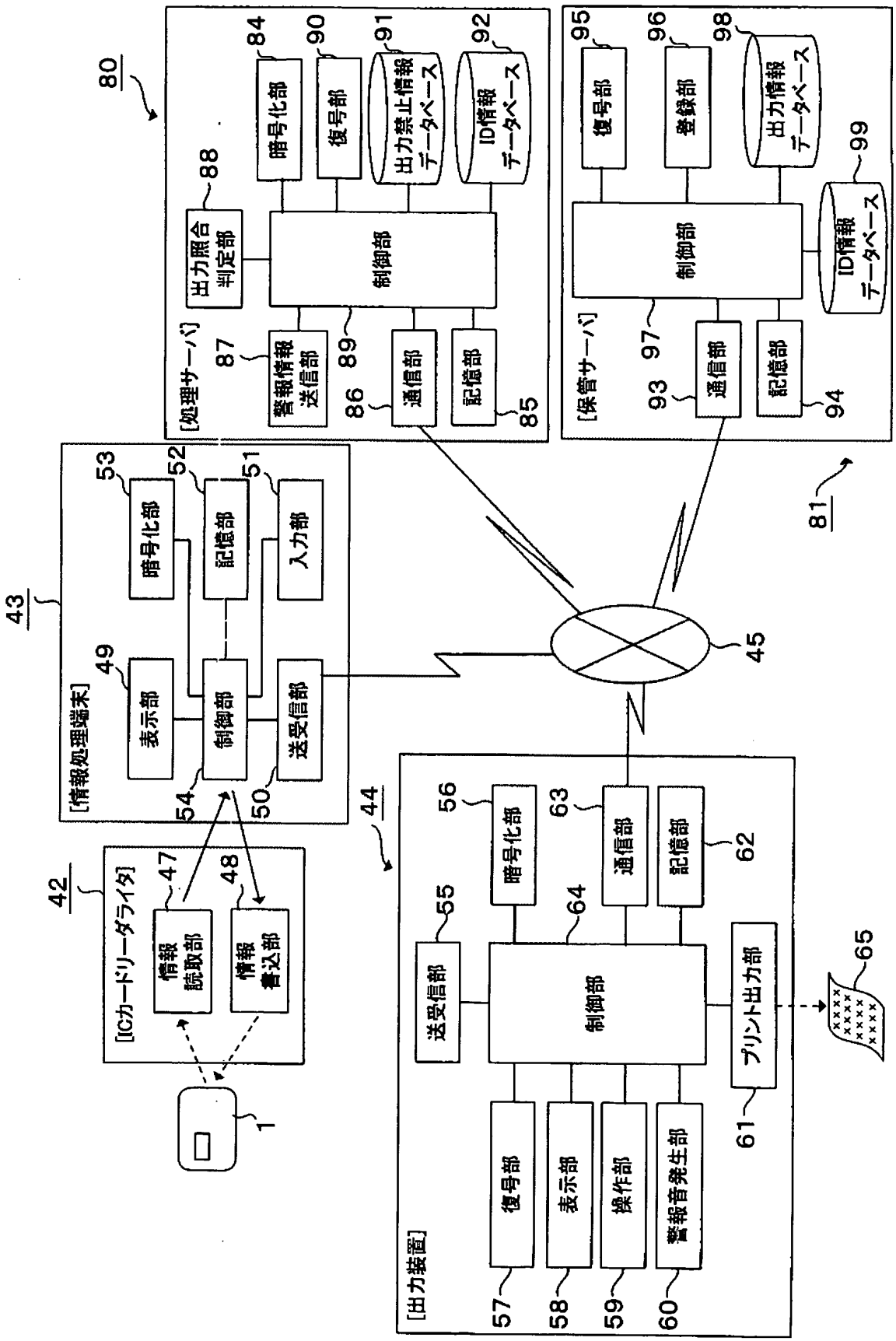
[図14]


スタート
ICカードリーダライターでICカードに記憶されているID情報と電子証明書を読み取る
S41
ICカードリーダライターで読み取った情報を情報処理端末に送る
S42
情報処理端末において、プリント出力させる情報と、ID情報をサーバとの間のSSLで共有したセッション鍵で暗号化させる
S43
暗号化された情報を情報処理端末からサーバに送る
S44
S45
復号した情報は、出力禁止情報か？
(YES)
(NO)
S46
サーバから情報処理端末に警報情報を送信し、処理を中止する
S47
サーバにおいて、プリント情報とID情報を紐つけて保管する
サーバにおいて、プリント情報を出力装置との間のSSLで共有したセッション鍵で暗号化する
S48
暗号化された情報を出力装置に送る
S49
出力装置において、受信した暗号化された情報をセッション鍵で復号する
S50
復号した情報を紙媒体に出力する
S51
エンド

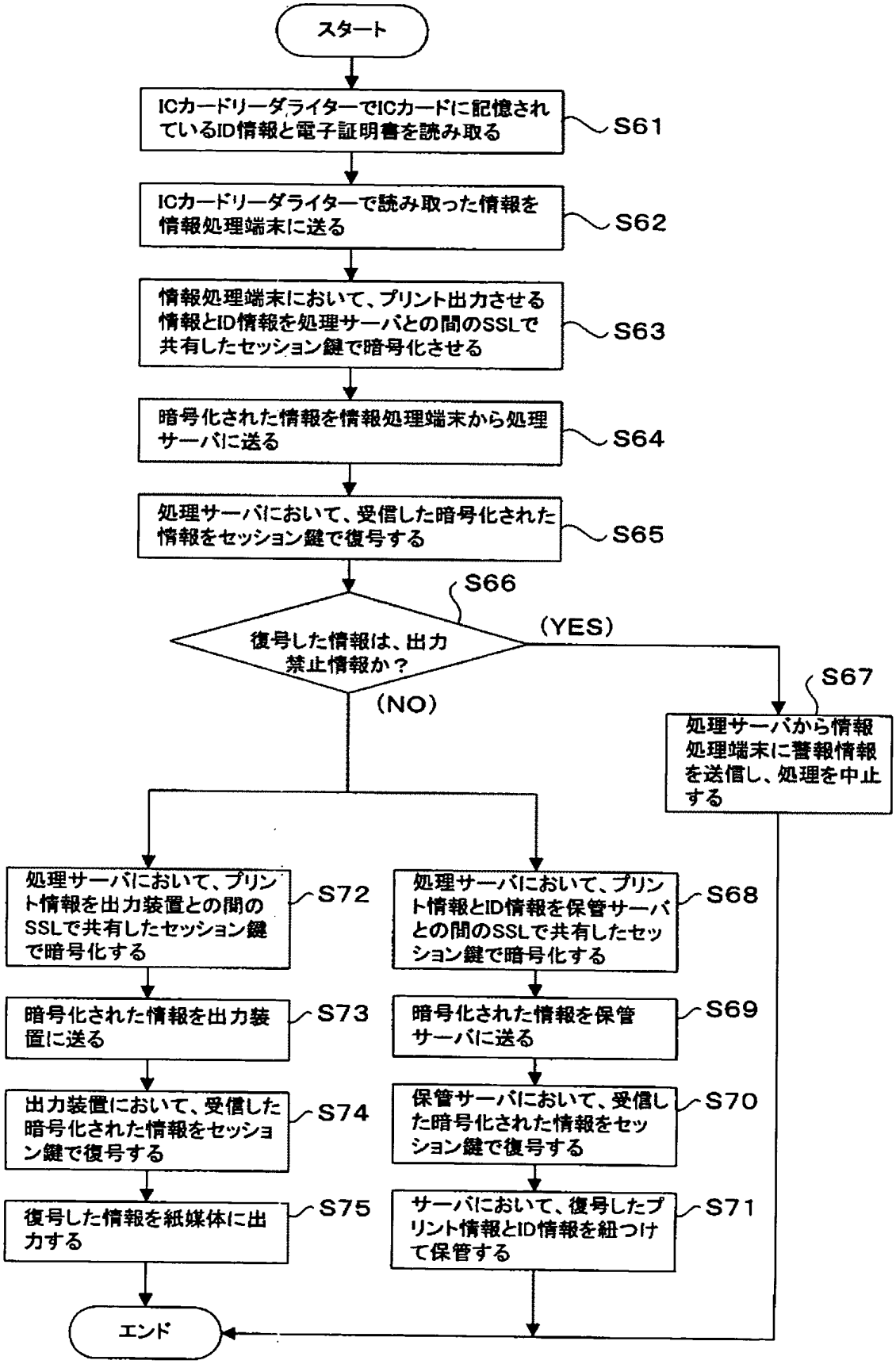
[図15]



[図16]


80
[処理サーバ]
84
暗号化部
90
復号部
91
出力禁止情報データベース
92
IDI情報データベース
88
出力照合判定部
制御部
87
警報情報送信部
89
86
通信部
85
記憶部
[保管サーバ]
95
復号部
96
整録部
98
出力情報データベース
99
IDI情報データベース
制御部
97
93
通信部
94
記憶部
81
43
[情報処理端末]
53
暗号化部
52
記憶部
51
入力部
49
表示部
制御部
送受信部
54
50
45
42
[ICカードリーダライタ]
47
情報読取部
48
情報書込部
1
44
[出力装置]
56
暗号化部
63
通信部
62
記憶部
55
送受信部
64
制御部
プリント出力部
65
61
復号部
表示部
操作部
警報音発生部
57
58
59
60

[図17]


スタート
ICカードリーダライターでICカードに記憶されているID情報と電子証明書を読み取る
S61
ICカードリーダライターで読み取った情報を情報処理端末に送る
S62
情報処理端末において、プリント出力させる情報とID情報を処理サーバとの間のSSLで共有したセッション鍵で暗号化させる
S63
暗号化された情報を情報処理端末から処理サーバに送る
S64
処理サーバにおいて、受信した暗号化された情報をセッション鍵で復号する
S65
S66
復号した情報は、出力禁止情報か？
(YES)
(NO)
S67
処理サーバから情報処理端末に警報情報を送信し、処理を中止する
処理サーバにおいて、プリント情報を出力装置との間のSSLで共有したセッション鍵で暗号化する
S72
暗号化された情報を出力装置に送る
S73
出力装置において、受信した暗号化された情報をセッション鍵で復号する
S74
復号した情報を紙媒体に出力する
S75
処理サーバにおいて、プリント情報とID情報を保管サーバとの間のSSLで共有したセッション鍵で暗号化する
S68
暗号化された情報を保管サーバに送る
S69
保管サーバにおいて、受信した暗号化された情報をセッション鍵で復号する
S70
サーバにおいて、復号したプリント情報とID情報を紐つけて保管する
S71
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/013956

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F3/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F3/12, H04N1/387, 1/40, B41J29/38, G03G21/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 00/51338 A (Matsushita Electric Industrial Co., Ltd.), 31 August, 2000 (31.08.00), Claims; Mode Nos. 1, 5, 7 & US 6807388 A	1-5,11,13 6-10,12,14
Y A	JP 7-49645 A (Ricoh Co., Ltd.), 21 February, 1995 (21.02.95), Full text; all drawings (Family: none)	1-5,11,13 6-10,12,14

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 December, 2004 (21.12.04)	11 January, 2005 (11.01.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/013956

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 9-44432 A (Fuji Xerox Co., Ltd.), 14 February, 1997 (14.02.97), Abstract; page 6, Par. No. [0041] to page 7, Par. No. [0050]; page 14, Par. Nos. [0114] to [0120]; page 17, Par. No. [0142] to page 20, Par. No. [0165] & EP 744695 A & US 5822533 A & DE 69622325 A	1-5,11,13 6-10,12,14
A	JP 6-22131 A (Minolta Camera Co., Ltd.), 28 January, 1994 (28.01.94), Abstract; all drawings (Family: none)	1-14
A	JP 7-212602 A (Ricoh Co., Ltd.), 11 August, 1995 (11.08.95), Abstract & US 5642199 A	1-14

国際調査[redacted]

国際出願番号 [redacted]T／ＪＰ２００４／０１３９５６

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl⁷ G06F 3／12

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl⁷ G06F 3／12，H04N 1／387，1／40
B41J 29／38，G03G 21／04

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００４年
日本国登録実用新案公報	１９９４－２００４年
日本国実用新案登録公報	１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	WO ００／５１３３８ Ａ（松下電器産業株式会社）２０００．０８．３１，特許請求の範囲、第１の実施形態、第５の実施形態、第７の実施形態＆ ＵＳ ６８０７３８８ Ａ	1-5, 11, 13 6-10, 12, 14
Y A	ＪＰ ７－４９６４５ Ａ（株式会社リコー）１９９５．０２．２１，全文、全図（ファミリーなし）	1-5, 11, 13 6-10, 12, 14
Y A	ＪＰ ９－４４４３２ Ａ（富士ゼロックス株式会社）１９９７．０２．１４，要約、第６頁【００４１】～第７頁【００５０】，第１４頁【０１１４】～【０１２０】，第１７頁【０１４２】～第２０頁【０１６５】＆ ＥＰ ７４４６９５ Ａ ＆ ＵＳ ５８２２５３３ Ａ ＆ ＤＥ ６９６２２３２５ Ａ	1-5, 11, 13 6-10, 12, 14

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 ２１．１２．２００４	国際調査報告の発送日 11. 1. 2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 山崎　慎一　　５Ｅ　９１７４ 電話番号　０３－３５８１－１１０１　内線　３５２０

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　６－２２１３１　Ａ（ミノルタカメラ株式会社）　１９９４．０１．２８，要約、全図（ファミリーなし）	１－１４
Ａ	ＪＰ　７－２１２６０２　Ａ（株式会社リコー）　１９９５．０８．１１，要約＆　ＵＳ　５６４２１９９　Ａ	１－１４